

On Multicasting Nested Message Sets over Combination Networks

Shirin Saeedi Bidokhti, Vinod M. Prabhakaran, and Suhas N. Diggavi,

Abstract

In this paper, we study delivery of two nested message sets over combination networks with an arbitrary number of receivers, where a subset of receivers (public receivers) demand only the lower priority message and a subset of receivers (private receivers) demand both the lower and the higher priority messages. We give a complete rate region characterization over combination networks with three public and many private receivers, where achievability is through linear coding. Our encoding scheme is general and characterizes an achievable region for arbitrary number of public and private receivers.

I. INTRODUCTION

The optimal rates with which one message set could be multicast to multiple destinations was established in the original work of Ahlswede *et al.* [1] and it was shown that performing network coding is necessary to achieve the capacity. Later, [2], [3], [4] showed that linear network coding is capacity achieving and [5] demonstrated randomized construction of multicast network codes.

The problem of delivering multiple messages is unresolved in general, though there has been progress on some special cases. In particular, [6], [7], [8] consider graphs with a single source and two destinations and characterize the capacity region for a common and two individual message sets. In [9], the capacity region of multicasting two nested message sets is derived over combination networks with three destinations.

In this paper, we study optimal encoding schemes for multicasting two nested message sets towards many destinations over a class of networks which are known as combination networks.

A combination network is a three-layer single source multi-terminal directed network, first introduced in [10] by Ngai and Yeung (See Figure 1). The class of combination networks turn out to be a rich class of networks in that it captures many of the inherent difficulties of general networks, while being simple enough to explore new coding schemes. Furthermore, they are among the simplest models for broadcast channels, where the media sharing is modeled via the common resources.

In this paper, we study delivery of two nested messages, the lower priority destined to all receivers and the higher priority destined to a subset of receivers.

II. PROBLEM FORMULATION AND MAIN RESULTS

A source communicates a common message W_1 of rate R_1 and a private message W_2 of rate R_2 towards K destinations over a combination network and the goal is that m (public) receivers indexed by $I_1 = \{1, 2, \dots, m\}$

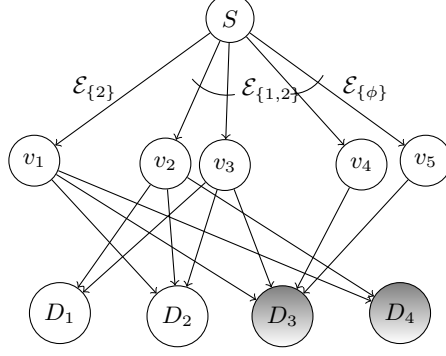


Fig. 1: A combination network with public receivers 1, 2 and private receivers 3, 4. Labeling of the resources is done w.r.t. public receivers, e.g. $\mathcal{E}_\phi = \{(s, v_4), (s, v_5)\}$, $\mathcal{E}_{\{1\}} = \{\}$, $\mathcal{E}_{\{2\}} = \{(s, v_1)\}$, $\mathcal{E}_{\{1,2\}} = \{(s, v_2), (s, v_3)\}$. Superscripts denote accessibility of resources to the private receivers, e.g., $\mathcal{E}_\phi^3 = \{(s, v_4), (s, v_5)\}$, $\mathcal{E}_\phi^4 = \{\}$, $\mathcal{E}_{\{1\}}^3 = \mathcal{E}_{\{1\}}^4 = \{\}$, $\mathcal{E}_{\{2\}}^3 = \mathcal{E}_{\{2\}}^4 = \{(s, v_1)\}$, $\mathcal{E}_{\{1,2\}}^3 = \{(s, v_3)\}$, $\mathcal{E}_{\{1,2\}}^4 = \{(s, v_2)\}$.

recover the common message and the rest $k - m$ (private) receivers indexed by $I_2 = \{m + 1, \dots, k\}$ recover both messages. The network over which communication takes place is a general combination network as depicted in Figure 1. All edges of the combination network are assumed to be carrying symbols from a finite field \mathbb{F} . The problem of interest is characterizing the ultimate rate pairs (R_1, R_2) at which messages W_1 and W_2 can be communicated reliably. We express all rates in terms of $\log_2 |\mathbb{F}|$.

Throughout this paper, we refer to the outgoing edges of the source as the *resources* of the combination network and we denote them by a set \mathcal{E} . We further identify these resources with respect to the public receivers they are connected to; i.e., we denote the set of all resources that are connected to every public receiver in $S \subseteq I_1$ and not connected to any public receiver not in S by $\mathcal{E}_S \subseteq \mathcal{E}$. Note that edges of set \mathcal{E}_S may or may not be connected to the private receivers. Whenever needed, however, we identify the subset of edges in \mathcal{E}_S that are also connected to a private receiver p , by \mathcal{E}_S^p . Figure 1 shows this notation over a combination network with four receivers.

For our use later, we define superset saturated subsets of 2^{I_1} as follows.

Definition 1 (superset saturated subsets). *We say that subset $\mathcal{T} \subseteq 2^{I_1}$ is superset saturated if it holds that S is an element of \mathcal{T} only if every $S' \supseteq S$ is an element of \mathcal{T} . In words, every set S in \mathcal{T} implies all its supersets, e.g. over subsets of $2^{\{1,2,3\}}$, $\mathcal{T} = \{\{1\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$ has prefix property, but not $\mathcal{T} = \{\{1\}, \{1,3\}, \{1,2,3\}\}$. For notational matters, we sometimes abbreviate a subset \mathcal{T} by the few sets that are not implied by the other sets in \mathcal{T} . For example, $\{\{1\}, \{1,2\}, \{1,3\}, \{1,2,3\}\}$ is abbreviated by $\{\{1\}\star\}$, and $\{\{1\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$ is abbreviated by $\{\{1\}\star, \{2,3\}\star\}$.*

To communicate messages W_1 and W_2 , each edge of the network carries signals containing information about messages W_1 and/or W_2 . We denote the signal carried over an edge e by X_e , which is a scalar from finite field \mathbb{F} . We denote by X_S , where $S \subseteq I_1$, the set of all signals carried over resource edges in \mathcal{E}_S , and by X_S^p , where $S \subseteq I_1$

and $p \in I_2$, the set of all signals carried over resource edges in \mathcal{E}_S^p . Similarly to simplify notation, we sometimes abbreviate the union sets $\bigcup_{S \in \mathcal{S}} \mathcal{E}_S$, $\bigcup_{S \in \mathcal{S}} \mathcal{E}_S^p$ and $\bigcup_{S \in \mathcal{S}} X_S$, by \mathcal{E}_S , \mathcal{E}_S^p and X_S respectively. The vector of all received signals at receiver $i \in \{1, \dots, K\}$ is denoted by Y_i , and it consists of all signals X_S , where $i \in S \subseteq I_1$. Finally when working with transmission blocks of length n , we use \bar{X} to denote signal X over a whole block.

We summarize the main result of this paper in the following theorems.

Theorem 1. Consider a combination network with m public receivers (indexed within $I_1 = \{1, \dots, m\}$) and $K - m$ private receivers (indexed within $I_2 = \{m + 1, \dots, K\}$). Given a large enough finite field \mathbb{F} , rate pair (R_1, R_2) is achievable if there exist α_S , $S \subseteq I_1$, such that

$$\begin{aligned} \alpha_S &\geq 0 & \forall \phi \neq S \subseteq I_1 \\ R_2 &= \sum_{S \subseteq I_1} \alpha_S \\ R_1 + \sum_{\substack{S \subseteq I_1 \\ S \ni i}} \alpha_S &\leq \sum_{\substack{S \subseteq I_1 \\ S \ni i}} |\mathcal{E}_S| \quad \forall i \in I_1 \\ R_2 &\leq \sum_{S \in \mathcal{T}} \alpha_S + \sum_{S \in \mathcal{T}^c} |\mathcal{E}_S^p| \quad \forall p \in I_2, \quad \forall \mathcal{T} \subseteq 2^{I_1} \text{ superset saturated} \\ R_1 + R_2 &\leq \sum_{S \subseteq I_1} |\mathcal{E}_S^p| \quad \forall p \in I_2 \end{aligned} \tag{1}$$

Theorem 2. Over a combination network with $m = 2$ public and many private receivers, any achievable rate pair lies in the rate region of Theorem II (for $I_1 = \{1, 2\}$, $I_2 = \{3, \dots, K\}$).

Theorem 3. Over a combination network with $m = 3$ public and many private receivers, any achievable rate pair lies in the rate region of Theorem II (for $I_1 = \{1, 2, 3\}$, $I_2 = \{4, \dots, K\}$).

III. RATE SPLITTING AND LINEAR ENCODING SCHEMES

Throughout this section, we confine ourselves to linear encoding at the source, and we always assume all rates to be non-negative integer values¹. Let $w_{1,1}, \dots, w_{1,R_1}$ and $w_{2,1}, \dots, w_{2,R_2}$ be variables in finite field \mathbb{F} for messages W_1 and W_2 respectively. We call them symbols of the common and the private message. Consider vector $W \in \mathbb{F}^{R_1+R_2}$ as the vector with coordinates in the standard basis $W = [w_{1,1} \dots w_{1,R_1} w_{2,1} \dots w_{2,R_2}]^T$.

We use linear coding as the encoding scheme at the source; i.e., after properly rearranging the signals that are sent over the resources of the combination network, X_S , $S \subseteq I_1$, we have

$$\begin{bmatrix} X_{\{1, \dots, m\}} \\ \vdots \\ X_{\{2\}} \\ X_{\{1\}} \\ X_\phi \end{bmatrix} = \mathbf{A} \cdot W,$$

where $\mathbf{A} \in \mathbb{F}^{|\mathcal{E}| \times (R_1+R_2)}$ is the encoding matrix. The aim of this section is to design \mathbf{A} so that the public receivers decode message W_1 and the private receivers decode both messages W_1, W_2 . We then characterize the region

¹There is no loss of generality in this assumption. One can deal with non-integer values R_1 and R_2 , by considering blocks of large enough length n , and working with (approximately) integer rates nR_1 and nR_2

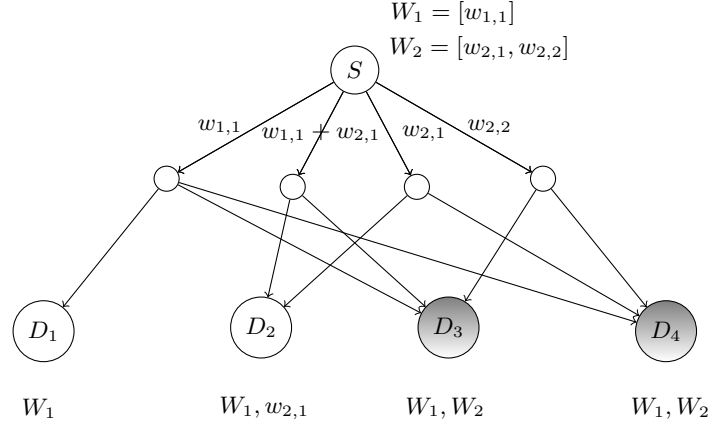


Fig. 2: Partial information about the private message needs to be revealed to public receiver D_2 in order to have rate pair $(R_1, R_2) = (1, 2)$ achievable

achievable by our code designs.

The challenge in optimal code design in this problem stems from the fact that destinations receive different subsets of the sent signals X_S , $S \subseteq I_1$, and have two different decodability concerns. On one hand, private receivers require their received signals to bring information about all information symbols of the common and the private message. On the other hand, public receivers might not be able to decode the common message if their received signals contain too much information about the private message. This tension is seen better through the following example.

Example 1. Consider the combination network shown in Figure 2, where the source communicates a common message $W_1 = [w_{1,1}]$ and a private message $W_2 = [w_{2,1}, w_{2,2}]$ to four receivers. Receivers 1 and 2 are public receivers and receivers 3 and 4 are private receivers. In this example, one can easily verify that (i) randomly linearly combining all information symbols and sending them out on the resources of the combination network allows neither of the public receivers decode their message of interest, and (ii) combining the information symbols across the two message sets is necessary to achieve rate pair $(1, 2)$. More precisely, rate pair $(1, 2)$ is feasible only if signal $X_{\{2\}}$ carries information about one symbol of message W_2 (or one linear combination out of the message space of W_2) in addition to common message W_1 .

Example 1 suggests that an optimal encoding scheme should allow mixing of the common message with the private message, but in a restricted and controlled manner so that it allows decodability of the common message at public receivers. Before attempting such a code design, let us find conditions for decodability of messages from received signals.

Lemma 1. *Let vector Y has the following construction*

$$Y = \left[\mathbf{T}_1 \mid \mathbf{T}_2 \right] \cdot \begin{bmatrix} W_1 \\ W_2 \end{bmatrix}, \quad (2)$$

where $\mathbf{T}_1 \in \mathbb{F}^{r \times R_1}$, $\mathbf{T}_2 \in \mathbb{F}^{r \times R_2}$, $W_1 \in \mathbb{F}^{R_1 \times 1}$, and $W_2 \in \mathbb{F}^{R_2 \times 1}$. Message W_1 is recoverable from Y if and only if $\text{rank}(\mathbf{T}_1) = R_1$ and the columns space of \mathbf{T}_1 is disjoint from that of \mathbf{T}_2 .

Proof: Let $Y = \mathbf{T}_1 W_1 + \mathbf{T}_2 W_2$ and $Y' = \mathbf{T}_1 W'_1 + \mathbf{T}_2 W'_2$. We prove that (1) if W_1 is recoverable from Y , then $\text{rank}(\mathbf{T}_1) = R_1$ and column spaces of \mathbf{T}_1 and \mathbf{T}_2 are disjoint, (2) if $\text{rank}(\mathbf{T}_1) = R_1$ and column spaces of \mathbf{T}_1 and \mathbf{T}_2 are disjoint, then W_1 is recoverable from Y .

We start by proving the first statement. Since W_1 is recoverable from Y , it holds for any W_1, W_2, W'_1, W'_2 that if $Y = Y'$ (or equivalently $\mathbf{T}_1(W_1 - W'_1) + \mathbf{T}_2(W_2 - W'_2) = 0$) then $W_1 = W'_1$. In particular for $W_2 = W'_2$, one derives that for any W_1, W'_1 , equation $\mathbf{T}_1(W_1 - W'_1) = 0$ results in $W_1 = W'_1$. Therefore \mathbf{T}_1 is column-wise fullrank; i.e., $\text{rank}(\mathbf{T}_1) = R_1$. Furthermore for all vectors W_2, W'_2 such that $\mathbf{T}_2(W_2 - W'_2) \neq 0$, one obtains $\mathbf{T}_1(W_1 - W'_1) \neq \mathbf{T}_2(W_2 - W'_2)$; i.e., columns space of matrix \mathbf{T}_2 is disjoint from the column space of matrix \mathbf{T}_1 .

To prove the second statement, we prove that if it holds that $\text{rank}(\mathbf{T}_1) = R_1$ and column spaces of \mathbf{T}_1 and \mathbf{T}_2 are disjoint, then equation $Y = Y'$ (or equivalently $\mathbf{T}_1(W_1 - W'_1) + \mathbf{T}_2(W_2 - W'_2) = 0$) results in $W_1 = W'_1$ for all vectors W_1, W_2, W'_1, W'_2 . We show this by contradiction. Let $\mathbf{T}_1(W_1 - W'_1) + \mathbf{T}_2(W_2 - W'_2) = 0$ and $W_1 \neq W'_1$. For the cases where $\mathbf{T}_2(W_2 - W'_2) = 0$, we get $\mathbf{T}_1(W_1 - W'_1) = 0$ for $W_1 \neq W'_1$, which contradicts the original assumption of $\text{rank}(\mathbf{T}_1) = R_1$. For other cases, equation $\mathbf{T}_1(W_1 - W'_1) + \mathbf{T}_2(W_2 - W'_2) = 0$ suggests that there exists at least one non-zero vector in the intersection of the column spaces of \mathbf{T}_1 and \mathbf{T}_2 which contradicts the second original assumption. ■

Corollary 1. *Messages W_1, W_2 are recoverable from Y in equation 2, if only if $\text{rank}([\mathbf{B}_1 | \mathbf{B}_2]) = R_1 + R_2$.*

Corollary 2. *Message W_1 is recoverable from Y in equation 2, only if $\text{rank}(\mathbf{B}_2) \leq r - R_1$.*

Since every receiver sees a subset of the sent signals, from corollary 1 and 2 it becomes clear that an admissible linear code need to satisfy many rank constraints on its different sub-matrices. In this paper, our primary approach to the design of such codes is through zero-structured matrices, as defined next.

A. Zero-structured matrices

Definition 2. A zero-structured matrix $\mathbf{T} \in \mathbb{F}^{r \times c}$ is a $2^t \times 2^t$ block matrix, indexed on rows and columns by subsets of $\{1, \dots, t\}$, such that block $b_{(T,S)} \in \mathbb{F}^{r_T \times c_S}$, $T, S \subseteq \{1, \dots, t\}$, is set to zero if $T \not\subseteq S$, and is indeterminate

otherwise. E.g., equation (3) demonstrates this definition for $t = 2$.

$$\mathbf{T} = \begin{array}{c} \begin{array}{cccc} \xleftrightarrow{c_{\{1,2\}}} & \xleftrightarrow{c_{\{1\}}} & \xleftrightarrow{c_{\{2\}}} & \xleftrightarrow{c_\phi} \\ \left[\begin{array}{|c|c|c|c|} \hline & 0 & 0 & 0 \\ \hline & & 0 & 0 \\ \hline & 0 & & 0 \\ \hline & & & \\ \hline \end{array} \right] & \begin{array}{l} \updownarrow r_{\{1,2\}} \\ \updownarrow r_{\{1\}} \\ \updownarrow r_{\{2\}} \\ \updownarrow r_\phi \end{array} \end{array} \end{array} \quad (3)$$

In this subsection we prove conditions for zero-structured matrices so that they can be filled column-fullrank.

Lemma 2. *Given a large enough finite field \mathbb{F} , a uniform random choice for the indeterminates of a zero-structured matrix $\mathbf{T} \in \mathbb{F}^{r \times c}$ (as specified in Definition 2) makes it column-fullrank (w.h.p.), provided that*

$$c \leq \sum_{S \in \mathcal{T}} c_S + \sum_{S \in \mathcal{T}^c} r_S \quad \forall \mathcal{T} \subseteq 2^{\{1, \dots, t\}} \text{ superset saturated} \quad (4)$$

We devote the rest of this subsection to proving this lemma, for it gives intuition and builds a background for the later proofs also. The proof is simple and the general idea is to reduce the problem of matrix \mathbf{T} being column-fullrank to an information flow unicast problem. For simplicity of notation and clarity of proofs, we give details of the proof for $t = 2$. It will become clear that the results hold in general.

In particular, let matrix $\mathbf{T} \in \mathbb{F}^{r \times c}$ be a zero-structured matrix given by equation (3). Lemma 3 reduces the problem of matrix \mathbf{T} being column-fullrank to an information flow unicast problem over the virtual network of Figure 3, and Lemma 4 finds conditions for feasibility of the equivalence unicast problem. Consider the network shown in Figure 3. Over this virtual network, a source node A wants to communicate a message of rate c to a sink node B . The thin edges of the network are of unit capacity, carrying symbols of finite field \mathbb{F} , and the thick edges are of infinite capacity. The network is tailored so that each intermediate node n_S , $S \subseteq \{1, \dots, t\}$, sends information only to nodes n'_T , where $T \subseteq S$. Such a structure closely relates this network to matrix \mathbf{T} , as we see in Lemma 3.

Lemma 3. *Given the zero-structured matrix $\mathbf{T} \in \mathbb{F}^{r \times c}$ of equation (3), the following three statements are equivalent.*

- (i) *A random choice of \mathbf{T} is with high probability column-fullrank*
- (ii) *A message of rate c could be unicast over the virtual network of Figure 3 from source node A to sink node B .*
- (iii) *There is a 0 – 1 assignment of matrix \mathbf{T} , given by a permutation of identity matrix $\mathbb{I}_{c \times c}$.*

Proof: Here, we only prove that statement (i) and statement (ii) are equivalent. Equivalency of (ii) and (iii) becomes clear from the proof, and we bring it in Appendix A.

(i) \Rightarrow (ii): Assume that matrix \mathbf{T} has all its indeterminates picked uniformly at random from finite field \mathbb{F} and is column-fullrank. Over the virtual network of Figure 3, we propose a network code that constitutes a transfer matrix (from node A to node B) exactly equal to the fullrank matrix \mathbf{T} : First, have each outgoing edge of the source carry one uncoded symbol of the message. Then, Let the first $r_{\{1,2\}}$ rows of matrix \mathbf{T} specify the local

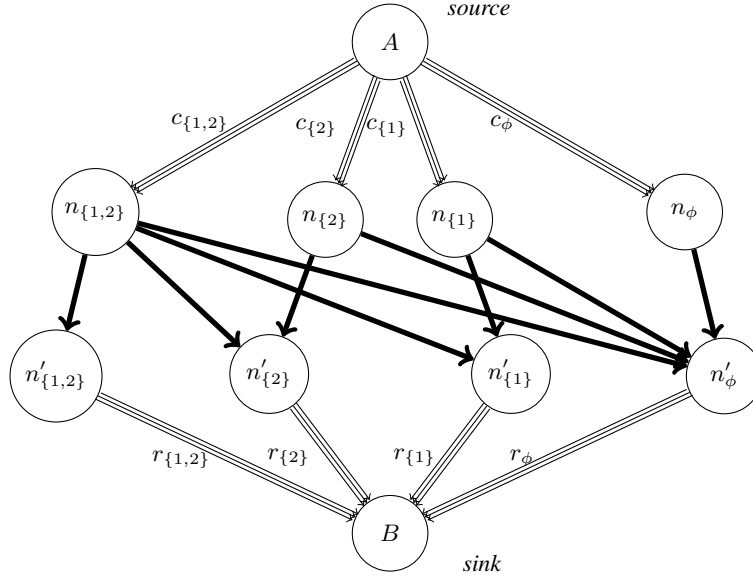


Fig. 3: Source node A communicates a message of rate $c = \sum_S s_S$ to the sink node, B .

encoding matrix at node $n'_{1,2}$. Similarly, let the second r_{2} , third r_{1} , and last r_{ϕ} set of rows of matrix \mathbf{T} specify the local encoding matrices at nodes n'_{2} , n'_{1} , and n'_{ϕ} , respectively. Note that the zero-structure of matrix \mathbf{T} , which is given in equation (3), ensures that this is a well defined construction. It follows that \mathbf{T} is the transfer matrix from node A to node B and since it is column-fullrank, the encoded message can be decoded at sink node B .

- (ii) \Rightarrow (i): If a message of rate c could be unicast over the virtual network of Figure 3 (from node A to node B), then its c symbols could be sent uncoded out of the source node A (since there is only one sink), and random linear network coding in the intermediate nodes ensures, with high probability, that the message is decodable at node B . This linear network code could be used, in the same manner as described above, to construct a (random) zero-structured matrix \mathbf{T} which is full-rank.

■

By Lemma 3, conditions under which matrix \mathbf{T} could be made full-rank is given by the min-cut between nodes A and B over the virtual network of Figure 3.

Lemma 4. *The min-cut separating nodes A and B over the virtual network of Figure 3 is given by the following expression.*

$$\min_{\substack{\mathcal{T} \subseteq 2^{I_1} \\ \mathcal{T} \text{ has prefix property}}} \sum_{S \in \mathcal{T}} c_S + \sum_{S \in \mathcal{T}^c} r_S \quad (5)$$

Proof: Consider all cuts separating source node A from sink node B . Since the intermediate edges all have

infinite capacity, the minimum cut does not contain any edges from them. One can easily verify the following over Figure 3: If an edge (n'_T, B) , $T \subseteq \{1, \dots, t\}$, does not belong to the cut, then all edges (A, n_S) where $S \supseteq T$ belong to that cut. So each (finite-valued) cut is derived for a set $\mathcal{S} \subseteq 2^{\{1, \dots, t\}}$ and has its value as

$$\sum_{S \in \mathcal{S}} r_S + \sum_{S \supseteq T, T \in \mathcal{S}^c} c_S. \quad (6)$$

It is not difficult to verify that the minimal cuts are derived for sets \mathcal{S}^c that have prefix property. Renaming \mathcal{S}^c as \mathcal{T} concludes the proof. ■

B. Zero-structured encoding schemes: an achievable region

We saw that the resources available to a public receiver should not contain too much information about the private message, in order to allow the common message be decoded. In our primary approach, we resolve this by a *zero-structured encoding matrix*. Equation (7) shows such an encoding matrix specified to two public and many private receivers. The non-zero entries are all indeterminate and to be designed appropriately. Also, parameters $\alpha_{\{1,2\}}$, $\alpha_{\{2\}}$, $\alpha_{\{1\}}$ and α_ϕ are non-negative structural parameters, and they satisfy $\alpha_{\{1,2\}} + \alpha_{\{2\}} + \alpha_{\{1\}} + \alpha_\phi = R_2$.

$$\mathbf{A} = \begin{array}{ccccc} & \xleftarrow{R_1} & \xleftrightarrow{\alpha_{\{1,2\}}} & \xleftrightarrow{\alpha_{\{2\}}} & \xleftrightarrow{\alpha_{\{1\}}} & \xleftrightarrow{\alpha_\phi} \\ \begin{bmatrix} & & & 0 & 0 & 0 \\ & & & & 0 & 0 \\ & & & 0 & & 0 \\ & & & & & \end{bmatrix} & \begin{array}{l} \updownarrow |\mathcal{E}_{\{1,2\}}| \\ \updownarrow |\mathcal{E}_{\{2\}}| \\ \updownarrow |\mathcal{E}_{\{1\}}| \\ \updownarrow |\mathcal{E}_\phi| \end{array} \end{array}. \quad (7)$$

In other words, matrix \mathbf{A} splits message W_2 into four message subsets, $W_2^{\{1,2\}}$, $W_2^{\{2\}}$, $W_2^{\{1\}}$, W_2^ϕ , of rates $\alpha_{\{1,2\}}$, $\alpha_{\{2\}}$, $\alpha_{\{1\}}$, α_ϕ respectively. The structure of \mathbf{A} ensures that only messages $W_2^{\{1,2\}}$ and $W_2^{\{1\}}$ are involved in linear combinations received at public receiver 1. Similarly, only messages $W_2^{\{1,2\}}$ and $W_2^{\{2\}}$ are involved in linear combinations received at public receiver 2.

More generally, we split message W_2 into all message subsets, W_2^S of rate α_S , $S \subseteq I_1$, such that

$$\sum_S \alpha_S = R_2, \quad (8)$$

and we use a zero-structured encoding matrix \mathbf{A} that allows W_2^S to be involved (only) in linear combinations that are sent over resources in \mathcal{E}_T where $T \subseteq S$. Refer to a zero-structured matrix \mathbf{A} , we sometimes also specify the rate split parameters α_S , $S \subseteq I_1$.

Through such an encoding, the received signals at each destination is given as follows. We ask if message(s) of interest are decodable.

- **Public receiver** $i \in I_1$: Received signal Y_i is the vector of all the signals carried by resources available to destination i ; e.g., using the (zero-structured) encoding matrix of equation (7) over a combination network

with two public receivers, we have Y_2 as follows.

$$Y_2 = \begin{bmatrix} X_{\{1,2\}} \\ X_{\{i\}} \end{bmatrix} = \begin{bmatrix} \xleftrightarrow{R_1} & \xleftrightarrow{\alpha_{\{1,2\}}} & \xleftrightarrow{\alpha_{\{2\}}} & \xleftrightarrow{\alpha_{\{1\}}} & \xleftrightarrow{\alpha_\phi} \\ \hline & & 0 & 0 & 0 \\ & & & 0 & 0 \end{bmatrix} \begin{matrix} \downarrow |\mathcal{E}_{\{1,2\}}| \\ \downarrow |\mathcal{E}_{\{2\}}| \end{matrix} \cdot \begin{bmatrix} W_1 \\ W_2 \end{bmatrix} \quad (9)$$

Generally, received signal Y_i is given by $Y_i = \mathbf{A}_i W$, where \mathbf{A}_i is a zero-structured matrix and has at most $\sum_{S \subseteq I_1, S \ni i} \alpha_S$ non-zero columns. We use Lemma 1 to find conditions for decodability of W_1 . If entries of \mathbf{A}_i are picked uniformly at random from finite field \mathbb{F} with a large enough field size, the first R_1 columns of \mathbf{A}_i will be w.h.p. fullrank, and the column space of the first R_1 and last R_2 columns of \mathbf{A}_i will be w.h.p. disjoint, provided that

$$\sum_{\substack{S \subseteq I_1 \\ S \ni i}} \alpha_S \leq \sum_{\substack{S \subseteq I_1 \\ S \ni i}} |\mathcal{E}_S| - R_1. \quad (10)$$

So the common message is decodable at public receiver i if inequality (10) holds, assuming the encoding matrix takes its non-zero variables uniformly at random (over finite field \mathbb{F}).

- **Private receiver $p \in I_2$:** Received signal Y_p is the vector of all the signals carried by resources in the sets \mathcal{E}_S^p , $S \subseteq I_1$; E.g., using the zero-structured encoding matrix of equation (7) over a combination network with two public receivers, we have received signal Y_p as follows.

$$Y_p = \begin{bmatrix} X_{\{1,2\}}^p \\ X_{\{1\}}^p \\ X_{\{2\}}^p \\ X_\phi^p \end{bmatrix} = \begin{bmatrix} \xleftrightarrow{R_1} & \xleftrightarrow{\alpha_{\{1,2\}}} & \xleftrightarrow{\alpha_{\{1\}}} & \xleftrightarrow{\alpha_{\{2\}}} & \xleftrightarrow{\alpha_\phi} \\ \hline & & 0 & 0 & 0 \\ & & & 0 & 0 \\ & & 0 & & 0 \end{bmatrix} \begin{matrix} \downarrow |\mathcal{E}_{\{1,2\}}^p| \\ \downarrow |\mathcal{E}_{\{1\}}^p| \\ \downarrow |\mathcal{E}_{\{2\}}^p| \\ \downarrow |\mathcal{E}_\phi^p| \end{matrix} \cdot \begin{bmatrix} W_1 \\ W_2 \end{bmatrix} \quad (11)$$

Generally, received signal Y_p is given by $Y_p = \mathbf{A}_p W$, where \mathbf{A}_p is zero-structured. To have messages W_1, W_2 decodable at private receiver p , matrix \mathbf{A}_p is required to be column-fullrank. By Lemma 2, a uniform random choice of variables in matrix \mathbf{A}_p makes it column-fullrank, provided that the following inequalities hold.

$$R_2 \leq \sum_{S \in \mathcal{T}} \alpha_S + \sum_{S \in \mathcal{T}^c} |\mathcal{E}_S^p| \quad \forall \mathcal{T} \subset 2^{I_1} \text{ superset saturated} \quad (12)$$

$$R_1 + R_2 \leq \sum_{S \subseteq I_1} |\mathcal{E}_S^p| \quad (13)$$

Inequalities (10),(12) and (13) provide us with constraints on parameters α_S , $S \subseteq I_1$, under which even a (uniform) random choice of zero-structured encoding matrix \mathbf{A} ensures receiver's decodability requirements. Under such constraints, therefore, there exists a zero-structured encoding matrix that satisfies all decodability requirements. Whether or not a rate pair (R_1, R_2) is achievable through this scheme can be posed as a feasibility problem in terms of parameters α_S , $S \subseteq I_1$. We summarize this achievable region in the following proposition.

Proposition 1. *Consider a combination network with many public receivers (indexed within set I_1) and many private receivers (indexed within set I_2). Given a large enough finite field \mathbb{F} , a rate pair (R_1, R_2) is achievable if*

there exist variables α_S , $S \subseteq I_1$, that satisfy

Structural constraints:

$$\alpha_S \geq 0 \quad \forall S \subseteq I_1 \quad (14)$$

$$R_2 = \sum_{S \subseteq I_1} \alpha_S \quad (15)$$

Decoding constraints at public receiver $i \in I_1$:

$$R_1 + \sum_{\substack{S \subseteq I_1 \\ S \ni i}} \alpha_S \leq \sum_{\substack{S \subseteq I_1 \\ S \ni i}} |\mathcal{E}_S| \quad (16)$$

Decoding constraints at private receiver $p \in I_2$:

$$R_2 \leq \sum_{S \in \mathcal{T}} \alpha_S + \sum_{S \in \mathcal{T}^c} |\mathcal{E}_S^p| \quad \forall \mathcal{T} \subset 2^{I_1} \text{ superset saturated} \quad (17)$$

$$R_1 + R_2 \leq \sum_{S \subseteq I_1} |\mathcal{E}_S^p| \quad (18)$$

Remark 1. Note that inequality (16) ensures only decodability of the common message, and not the superposed messages, W_2^S , $i \in S \subseteq I_1$ (which are not of particular interest to the public receivers). To have public receiver i decode all private message subsets W_2^S , $i \in S \subseteq I_1$, one needs further constraints on α_S , as given in (19)².

$$\sum_{\substack{S \subseteq I_1 \\ S \ni i}} \alpha_S \leq \sum_{S \in \mathcal{T}} \alpha_S + \sum_{\substack{S \in \mathcal{T}^c \\ S \ni i}} |\mathcal{E}_S| \quad \mathcal{T} \subseteq \{\{i\}^*\} \text{ superset saturated} \quad (19)$$

Proposition 1 characterizes an achievable region, using standard techniques of rate splitting and linear superposition coding. We prove in Subsection IV-B that this encoding scheme is rate-optimal for combination networks with two public and many private receivers. Nonetheless, this encoding scheme is not in general optimal. We discuss this sub-optimality next and modify the encoding scheme to attain a strictly larger rate region.

C. Modified encoding schemes: an achievable region

We start by a combination network example, where linear superposition coding, as discussed, performs sub-optimally.

Example 2. Consider combination network of Figure 4 where destinations 1, 2, 3 are public receivers and destinations 4, 5, 6 are private receivers. It is clear that rate pair $(R_1 = 0, R_2 = 2)$ is achievable (just multicast the private message towards the private receivers using random linear network coding). However, there is no choice of $\alpha_S \geq 0$, $S \subseteq \{1, 2, 3\}$, which satisfies inequalities (14)-(18) for this rate pair, unless α_ϕ is allowed to be negative. One such set of parameters α_S is given by $\alpha_\phi = -1$, $\alpha_{\{1\}} = \alpha_{\{2\}} = \alpha_{\{3\}} = 1$, and $\alpha_{\{1,2\}} = \alpha_{\{1,3\}} = \alpha_{\{2,3\}} = \alpha_{\{1,2,3\}} = 0$.

²More precisely, call \mathbf{T}_i the submatrix of \mathbf{A}_i which does not contain the all-zero columns. One observes that messages W_2^S , $i \in S \subseteq I_1$, are all decodable if and only if \mathbf{T}_i is column-fullrank. Since \mathbf{T}_i is zero-structured, Lemma 2 gives the required constraints.

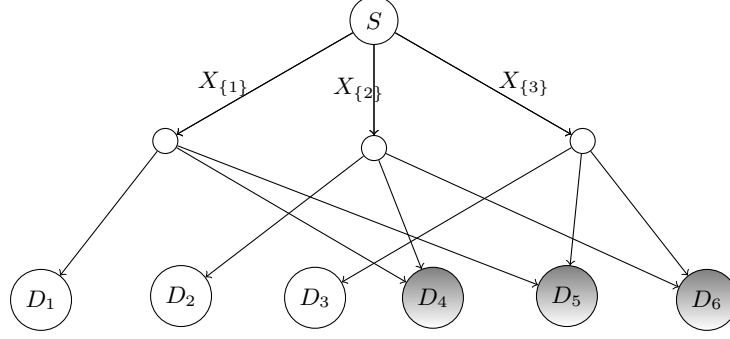


Fig. 4: Innerbound of Proposition 1 is not tight for more than two public receivers

Obviously, there is no longer a "structural" meaning to this negative parameter. Nonetheless, it still has a peculiar meaning that we try to investigate in this example. As suggested by the positive parameters $\alpha_{\{1\}}$, $\alpha_{\{2\}}$, $\alpha_{\{3\}}$, we would like to reveal a subspace of dimension one (of the private message space) to each public receiver. The subtlety comes in when one notices that these three subspaces will have to span each other, for message space of W_2 has a dimension of 2.

We use this observation to modify the encoding scheme and achieve rate pair $(0, 2)$. First pre-encode message W_2 , through a random pre-encoding matrix $\mathbf{P} \in \mathbb{F}^{3 \times 2}$, into a pseudo private message W'_2 . Then, encode W'_2 using a random zero-structured encoding matrix, as follows.

$$\begin{bmatrix} X_{\{1\}} \\ X_{\{2\}} \\ X_{\{3\}} \end{bmatrix} = \begin{bmatrix} & 0 & 0 \\ 0 & & 0 \\ 0 & 0 & \end{bmatrix} \begin{bmatrix} w'_{2,1} \\ w'_{2,2} \\ w'_{2,3} \end{bmatrix}$$

Notice that this zero-structured encoding matrix does reveal a subspace of dimension one (of the pseudo-private message space) to each public receiver. Furthermore, using such a pre-encoding/encoding scheme, each private receiver gets to decode two symbols out of the three symbols of W'_2 and can, therefore, decode the (original) private message W_2 w.h.p.

Inspired by example 2, we modify the basic encoding scheme, using an appropriate pre-encoder, to obtain a strictly larger achievable region as expressed in Theorem 1.

Theorem 1. Consider a combination network with many public receivers (indexed within a set I_1) and many private receivers (indexed within a set I_2). A rate pair (R_1, R_2) is achievable if there exist variables α_S , $S \subseteq I_1$, that satisfy

Structural constraints:

$$\alpha_S \geq 0 \quad \forall \phi \neq S \subseteq I_1 \quad (20)$$

$$R_2 = \sum_{S \subseteq I_1} \alpha_S \quad (21)$$

Decoding constraints at public receiver $i \in I_1$:

$$R_1 + \sum_{\substack{S \subseteq I_1 \\ S \ni i}} \alpha_S \leq \sum_{\substack{S \subseteq I_1 \\ S \ni i}} |\mathcal{E}_S| \quad (22)$$

Decoding constraints at private receiver $p \in I_2$:

$$R_2 \leq \sum_{S \in \mathcal{T}} \alpha_S + \sum_{S \in \mathcal{T}^c} |\mathcal{E}_S^p| \quad \forall \mathcal{T} \subseteq 2^{I_1} \text{ superset saturated} \quad (23)$$

$$R_1 + R_2 \leq \sum_{S \subseteq I_1} |\mathcal{E}_S^p| \quad (24)$$

Proof:

Let (R_1, R_2) be in the rate region of Theorem 1; i.e., there exist parameters α_S , $S \subseteq I_1$, that satisfy inequalities (20)-(24). Since we already know what to do if $\alpha \geq 0$, in this proof we emphasize more on $\alpha_\phi < 0$. In the following, we assume $(\alpha_\phi)^- = \min(0, \alpha_\phi)$ and $(\alpha_\phi)^+ = \max(0, \alpha_\phi)$.

First of all, pre-encode message W_2 into a message vector W'_2 of dimension $R_2 - (\alpha_\phi)^-$, through a random pre-encoding matrix $\mathbf{P} \in \mathbb{F}^{R_2 - (\alpha_\phi)^- \times R_2}$; i.e., we have

$$W'_2 = \mathbf{P}W_2. \quad (25)$$

Then, encode messages W_1 and W'_2 into the outgoing signals, using a random zero-structured matrix with rate split parameters α_S , $\phi \neq S \subseteq I_1$, with no column corresponding to $\alpha_\phi < 0$. The encoding matrix is therefore given as follows, where all indeterminates are picked uniformly at random from finite field \mathbb{F} .

$$\mathbf{A} = \begin{array}{c} \begin{array}{ccccc} \xleftrightarrow{R_1} & \xleftrightarrow{\alpha_{\{1,2\}}} & \xleftrightarrow{\alpha_{\{1\}}} & \xleftrightarrow{\alpha_{\{2\}}} & \xleftrightarrow{(\alpha_\phi)^+} \\ \hline & & 0 & 0 & 0 \\ \hline & & & 0 & 0 \\ \hline & & 0 & & 0 \\ \hline & & & & \end{array} & \begin{array}{l} \updownarrow |\mathcal{E}_{\{1,2\}}| \\ \updownarrow |\mathcal{E}_{\{1\}}| \\ \updownarrow |\mathcal{E}_{\{2\}}| \\ \updownarrow |\mathcal{E}_\phi| \end{array} \end{array} \cdot \begin{bmatrix} I_{R_1 \times R_1} & 0 \\ 0 & \mathbf{P} \end{bmatrix} \quad (26)$$

The condition for decodability of W_1 at each public receiver $i \in I_1$ is (22) and at each private receiver $p \in I_2$ is (24). This follows as before, from Lemma 1. All receivers can, therefore, decode the common message w.h.p. Promised by Lemma 5 which follows, private receivers can decode w.h.p. the private message also.

Lemma 5. *Given a large enough finite field \mathbb{F} , a uniform random assignment for variables in \mathbf{A} (over finite field \mathbb{F}) lets receiver p decode message W_2 w.h.p., provided that message W_1 is decoded and inequalities in (23) hold.*

We argued that the random encoding matrix of (26) let all destinations receive their message(s) of interest. Therefore, there exists such a linear encoding matrix that achieves rate pair (R_1, R_2) . ■

The achievable schemes we discussed in this section turn out to be optimal when there are few public and many private receivers. More precisely, we show in Section IV that

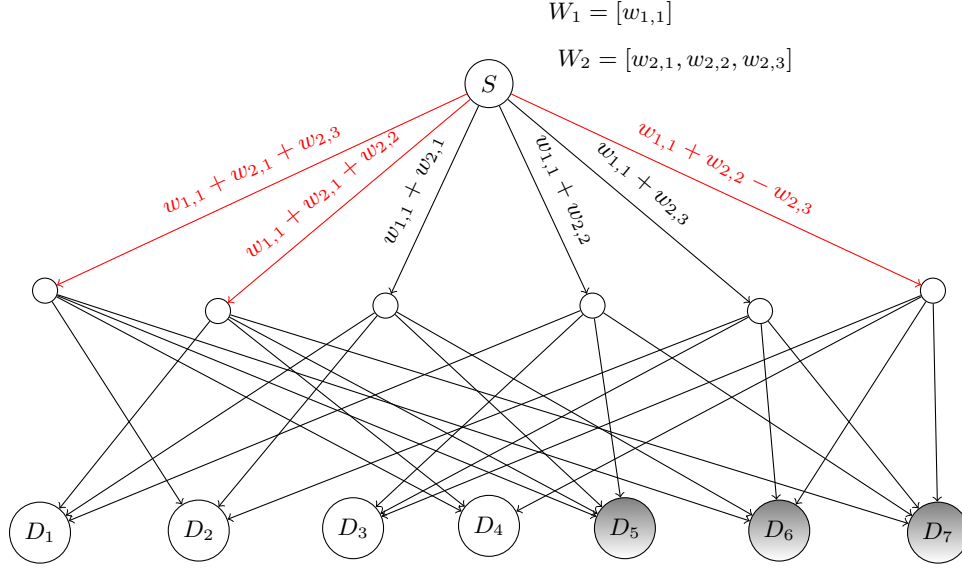


Fig. 5: Innerbound of Theorem 1 is not tight for more than three common receivers

- Innerbound of Theorem 1 coincides with that of Proposition 1 for $I_1 = \{1, 2\}$, $I_2 = \{2, \dots, K\}$, and is tight in such cases.
- Innerbound of Theorem 1 is tight for all cases with $m \leq 3$ public and many private receivers.

We close this section by an example which shows that the inner-bound of Theorem 1 is not tight in general.

Example 3. Consider the combination network depicted in Figure 5 over which s source intends to communicate messages W_1 and W_2 with rates $R_1 = 1$ and $R_2 = 3$ respectively. In this example, receivers 1, 2, 3, 4 are public and receivers 5, 6, 7 are private receivers. The encoding scheme which is shown on Figure 5 proves achievability of rate pair $(1, 3)$. However if one tries to use Theorem 1, it becomes clear that there exists no set of α_S , $S \subseteq I_1 = \{1, \dots, 4\}$, for which inequalities (20)-(24) all hold, unless the non-negativity constraints in (20) get relaxed.

To give an intuitive explanation on why our modified encoding scheme is not optimal in this example and what difficulty is hidden in constructing general optimal encoding schemes, consider combination network of Figure 5. We focus on the three red resources, which are all the resources that are available to public receiver 4. Since public receiver 4 needs to decode only the common message (which is of rate 1), no more than two dimensions of the private message could be involved in its received linear combinations. Now observe that these three resources repeat the exact same structure of Figure 4! More precisely, the allowed private rate on these resources is 2 and each resource is connected to one of public receivers 1, 2, 3, and two of the private receivers 5, 6, 7 (besides receiver 4). For reasons similar to example 2, a further random encoding is needed among the allowed two dimensions of the private message, finer than the global random pre-encoding that we performed.

IV. OPTIMALITY RESULTS

In this Section, we prove optimality results. More precisely, we prove optimality of the zero-structured encoding scheme of Subsection III-B when $I_1 = \{1, 2\}$, $I_2 = \{3, \dots, K\}$, and optimality of the modified encoding scheme of Subsection III-C when $I_1 = \{1, 2, 3\}$, $I_2 = \{4, \dots, K\}$. This is summarized in the following theorems.

Theorem 2. *Over a combination network with $m = 2$ public and many private receivers, any achievable rate pair lies in the rate region of Proposition 1/Theorem 1 (for $I_1 = \{1, 2\}$, $I_2 = \{3, \dots, K\}$).*

Theorem 3. *Over a combination network with $m = 3$ public and many private receivers, any achievable rate pair lies in the rate region of Theorem 1 (for $I_1 = \{1, 2, 3\}$, $I_2 = \{4, \dots, K\}$).*

A. Explicit projection of the polyhedron: proof to Theorem 2

Theorem 2 gives an outer-bound on the rate region that matches inner-bound of Proposition 1 when $m = 2$. Note that any rate pair in the rate region of Proposition 1 lies also in the rate region of Theorem 1. To prove this theorem, we first eliminate all parameters α_S , $S \subseteq I_1$, in rate region of Proposition 1, using Fourier-Motzkin method and obtain the following region (recall that $I_1 = \{1, 2\}$ and $I_2 = \{3, \dots, K\}$):

$$R_1 \leq \min\{|\mathcal{E}_{\{1\}}| + |\mathcal{E}_{\{1,2\}}|, |\mathcal{E}_{\{2\}}| + |\mathcal{E}_{\{1,2\}}|\} \quad (27)$$

$$R_1 + R_2 \leq \min_{p \in I_2} |\mathcal{E}_\phi^p| + |\mathcal{E}_{\{1\}}^p| + |\mathcal{E}_{\{2\}}^p| + |\mathcal{E}_{\{1,2\}}^p| \quad (28)$$

$$2R_1 + R_2 \leq \min_{p \in I_2} |\mathcal{E}_{\{1\}}| + |\mathcal{E}_{\{1,2\}}| + |\mathcal{E}_{\{2\}}| + |\mathcal{E}_{\{1,2\}}| + |\mathcal{E}_\phi^p| \quad (29)$$

We now prove that any achievable rate pair satisfies the three inequalities above. Inequalities (27) and (28) are intuitive (using cut set bounds) and are easy to derive. Inequality (29) is, however, not intuitive and we prove it in the following. Assume communication over block of length n , and denote by \bar{X} , collection of signals X within the communication block length. Let $\epsilon > 0$ be arbitrarily chosen. Then, R_2 is bounded as follows for each private receiver $p \in I_2$.

$$nR_2 \leq H(W_2|W_1) \quad (30)$$

$$\leq H(W_2|W_1) \pm H(W_2|W_1, \bar{Y}_p) \quad (31)$$

$$\stackrel{(a)}{\leq} I(W_2; \bar{Y}_p|W_1) + n\epsilon \quad (32)$$

$$\leq H(\bar{Y}_p|W_1) + n\epsilon \quad (33)$$

$$\stackrel{(b)}{\leq} H(\bar{X}_{\{\{1\}, \{1,2\}\}}^p, \bar{X}_{\{\{1\}, \{2\}, \{1,2\}\}}|W_1) + n\epsilon \quad (34)$$

$$\leq H(\bar{X}_{\{\{1\}, \{1,2\}\}}|W_1) + H(\bar{X}_{\{\{2\}, \{1,2\}\}}|W_1) + H(\bar{X}_{\{\{1\}, \{1,2\}\}}^p|\bar{X}_{\{\{1\}, \{2\}, \{1,2\}\}}, W_1) + n\epsilon \quad (35)$$

$$\stackrel{(c)}{\leq} H(\bar{X}_{\{\{1\}, \{1,2\}\}}) + H(\bar{X}_{\{\{2\}, \{1,2\}\}}) - 2nR_1 + H(\bar{X}_{\{\{1\}, \{1,2\}\}}^p|\bar{X}_{\{\{1\}, \{2\}, \{1,2\}\}}, W_1) + 3n\epsilon \quad (36)$$

$$\stackrel{(d)}{\leq} H(\bar{X}_{\{\{1\}, \{1,2\}\}}) + H(\bar{X}_{\{\{2\}, \{1,2\}\}}) - 2nR_1 + H(\bar{X}_\phi^p) + 3n\epsilon \quad (37)$$

$$\stackrel{(e)}{\leq} n(|\mathcal{E}_{\{1\}}| + |\mathcal{E}_{\{1,2\}}|) + n(|\mathcal{E}_{\{2\}}| + |\mathcal{E}_{\{1,2\}}|) - 2R_1 + n(|\mathcal{E}_\phi^p|) + 3n\epsilon \quad (38)$$

In the above chain of inequalities, step (a) follows by Fano's inequality. Step (b) follows because received signal \bar{Y}_p is given by the union $\bar{X}_{\{\{\},\{1\},\{2\}\{1,2\}\}}^p$ and we further provide the entropy term with the information of signals $\bar{X}_{\{1,2\}}, \bar{X}_{\{1\}}, \bar{X}_{\{1\}}$. Step (c) follows by Fano's inequality because for any achievable code, message W_1 should be decodable from $\bar{X}_{\{\{1\},\{1,2\}\}}$ or $\bar{X}_{\{\{1\},\{1,2\}\}}$. More precisely,

$$H(\bar{X}_{\{\{1\},\{1,2\}\}}|W_1) = H(\bar{X}_{\{\{1\},\{1,2\}\}}, W_1) - nR_1 \quad (39)$$

$$= H(\bar{X}_{\{\{1\},\{1,2\}\}}) + H(W_1|\bar{X}_{\{\{1\},\{1,2\}\}}) - nR_1 \quad (40)$$

$$\leq H(\bar{X}_{\{\{1\},\{1,2\}\}}) + n\epsilon - nR_1, \quad (41)$$

and similarly $H(\bar{X}_{\{\{2\},\{1,2\}\}}|W_1) \leq H(\bar{X}_{\{\{2\},\{1,2\}\}}) - nR_1 + n\epsilon$. Step (d) follows by the fact that \bar{X}_S^p is contained in \bar{X}_S for any $S \subseteq I_1$ (by definition) and the fact that by removing the conditioning in the entropy term, we increase it. Finally, step (e) follows by cardinality bound on entropy.

B. Sub-modularity of entropy function: proof to Theorem 3

While it was not difficult to eliminate all parameters α_S , $S \subseteq I_1$, from the rate region characterization when $m = 2$, this becomes computationally intractable when the number of public receivers increases. In this section, we prove Theorem 3, which gives an outer-bound on the rate region that matches inner-bound of Theorem 1 when $m = 3$. We bypass the issue of explicitly eliminating all parameters α_S , $S \subseteq I_1$, by first proving an outer-bound which looks *similar* to the inner-bound and then using sub-modularity to conclude the proof.

We start by an example.

Example 4. We ask if rate pair $(1, 2)$ is achievable over the combination network of figure 6 where $I_1 = \{1, 2, 3\}$ and $I_2 = \{4, 5\}$. To answer this question, let us first see if this rate pair is within inner-bound of Theorem 1. By solving the feasibility problem defined in inequalities (20)-(24) using Fourier-Motzkin method, one obtains the following inner-bound inequality, and concludes that rate pair $(1, 2)$ is not within inner-bound of Theorem 1.

$$4R_1 + 2R_2 \leq 7. \quad (42)$$

Once this is established, one can also answer to the following question: What linear combination of inequalities in (20)-(24) gave rise to this inner-bound inequality? For instance, here the answer is that summing two copies of constraint (22) (for $i = 1$), one copy of constraint (22) (for $i = 2$), one copy of constraint (22) (for $i = 3$), one copy of constraint (23) (for $\mathcal{T} = \{\{1\}\star, \{2, 3\}\star\}$), one copy of constraint (23) (for $\mathcal{T} = \{\{1\}\star, \{2\}\star, \{3\}\star\}$), and finally one copy of non-negativity constraint (20) (for $S = \{1, 2, 3\}$) gives rise to $4R_1 + 2R_2 \leq 7$.

We now write the following upper-bounds on R_1 and R_2 (which we prove in details in Subsection IV-B2). Notice the similarity of each outer-bound constraint in (43)-(48) to an inner-bound constraints that played role in derivation

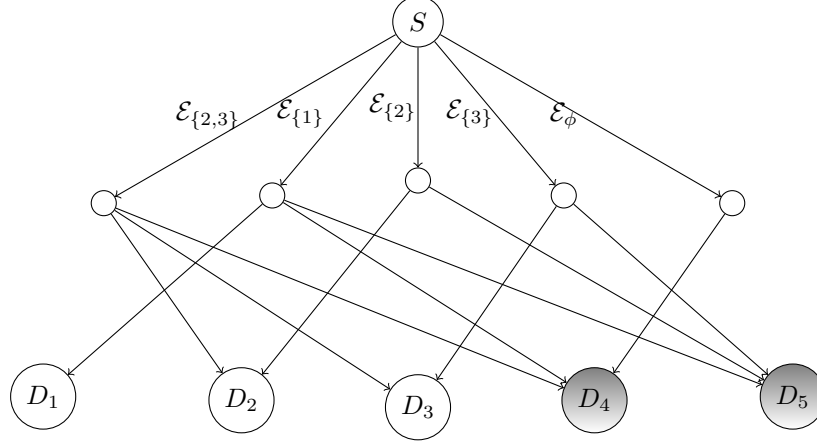


Fig. 6: Is $(1, 2)$ achievable over this combination network?

of $4R_1 + 2R_2 \leq 7$.

$$R_1 + \frac{1}{n} H(\bar{X}_{\{\{1\}\star\}} | W_1) \leq 1 \quad (43)$$

$$R_1 + \frac{1}{n} H(\bar{X}_{\{\{2\}\star\}} | W_1) \leq 2 \quad (44)$$

$$R_1 + \frac{1}{n} H(\bar{X}_{\{\{3\}\star\}} | W_1) \leq 2 \quad (45)$$

$$R_2 \leq \frac{1}{n} H(\bar{X}_{\{\{1\}\star, \{2,3\}\star\}} | W_1) + 1 \quad (46)$$

$$R_2 \leq \frac{1}{n} H(\bar{X}_{\{\{1\}\star, \{2\}\star, \{3\}\star\}} | W_1) \quad (47)$$

$$0 \leq \frac{1}{n} H(\bar{X}_{\{1,2,3\}} | W_1) \quad (48)$$

Take similar copies of these outer-bound constraints and sum them up to yield an outer-bound inequality of the following form. Note that among all resources only \mathcal{E}_ϕ , $\mathcal{E}_{\{1\}}$, $\mathcal{E}_{\{2\}}$, $\mathcal{E}_{\{3\}}$, $\mathcal{E}_{\{2,3\}}$ are non-empty.

$$4R_1 + 2R_2 \leq 7 - \frac{1}{n} \begin{pmatrix} 2H(\bar{X}_{\{1\}} | W_1) + H(\bar{X}_{\{2\}}, \bar{X}_{\{2,3\}} | W_1) + H(\bar{X}_{\{2,3\}}, \bar{X}_{\{3\}} | W_1) \\ -H(\bar{X}_{\{1\}}, \bar{X}_{\{2,3\}} | W_1) - H(\bar{X}_{\{1\}}, \bar{X}_{\{3\}}, \bar{X}_{\{2,3\}}, \bar{X}_{\{2\}} | W_1) \end{pmatrix} \quad (49)$$

$$\stackrel{(a)}{\leq} 7, \quad (50)$$

where (a) holds by sub-modularity.

The intuition from example (4) gives us a method to prove the converse to Theorem 1 for $I_1 = \{1, 2, 3\}$, $I_2 = \{4, \dots, K\}$. Before presenting the proof, let us introduce a few techniques, as it may not be clear how sub-modularity could be used in its generality.

1) *Sub-modularity, notation, convention:* We recall some definitions and results from [11]. Let $[\mathcal{M}]$ be a family of multi-sets of subsets of elements $\{1, \dots, N\}$. Given a multi-set $\mathcal{A} = \{A_1, \dots, A_l\} \in [\mathcal{M}]$, let multi-set \mathcal{A}' be obtained from \mathcal{A} by replacing A_i and A_j by $A_i \cap A_j$ and $A_i \cup A_j$. Multi-set \mathcal{A}' is then said to be an *elementary*

compression of \mathcal{A} . The elementary compression is, in particular, *non-trivial* if neither $A_i \subseteq A_j$ nor $A_j \subseteq A_i$. A sequence of elementary compressions gives a *compression*. A partial order \geq is defined over $[\mathcal{M}]$ as follows. $\mathcal{A} \geq \mathcal{B}$ if \mathcal{B} is a compression of \mathcal{A} (= iff the compression is composed of all trivial elementary compressions). Let $X = (X_i)_{i=1}^N$ be a sequence of random variables with $H(X)$ finite and let \mathcal{A} and \mathcal{B} be finite multi-sets of subsets of $\{1, \dots, N\}$ such that $\mathcal{A} \geq \mathcal{B}$. A simple consequence of the sub-modularity of the entropy function is $\sum_{A \in \mathcal{A}} H(X_A) \geq \sum_{B \in \mathcal{B}} H(X_B)$ [11, Theorem 5].

In this context, we consider $[\mathcal{M}]$ to be a family of multi-sets of subsets of 2^{I_1} , where $I_1 = \{1, 2, 3\}$. We denote multi-sets by bold calligraphic capital letters (e.g., \mathcal{A} and \mathcal{B}), sets of subsets of 2^{I_1} by calligraphic capital letters (e.g., \mathcal{A}_i , \mathcal{S} and \mathcal{T}), and subsets of 2^{I_1} by capital letters (e.g., S and T). We define *multi-sets of saturated pattern* and *multi-sets of standard pattern* as follows.

Definition 3 (Multiset of (superset) saturated pattern). *A multi-set (of subsets of 2^{I_1}) is said to be of (superset) saturated pattern if all its elements are superset saturated. E.g., $[\{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}]$ and $[\{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}, \{\{2, 3\}\}]$ are both of saturated pattern, but not $[\{\{2\}, \{1, 2\}, \{1, 2, 3\}\}]$ and $[\{\{1\}, \{2\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}, \{\{1\}, \{1, 2\}\}]$.*

Definition 4 (Multi-set of standard pattern). *A multi-set (of subsets of 2^{I_1}) is said to be of standard pattern if its elements are all of the form $\{S \subseteq I_1 : S \ni i\}$, for some $i \in I_1$. E.g., $[\{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}]$ and $[\{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}, \{\{2\}, \{1, 2\}, \{2, 3\}, \{1, 2, 3\}\}]$ are both multi-sets of standard pattern, but not $[\{\{1, 2\}, \{1, 2, 3\}\}]$ and $[\{\{1\}, \{2\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}]$.*

We say that multi-sets \mathcal{A} and \mathcal{B} are *balanced* if $\sum_{T \in \mathcal{A}} \mathbf{1}_{S \in T} = \sum_{T \in \mathcal{B}} \mathbf{1}_{S \in T}$, for all sets $S \in 2^{I_1}$.

One observes that (i) multi-sets of standard pattern are also of saturated pattern, (ii) The set of all multi-sets of saturated pattern is closed under compression (iii) if multi-set \mathcal{B} is a compression of multi-set \mathcal{A} , then they are balanced.

Let us look at inequality (50) in this formulation. Let $[\mathcal{M}]$ be a family of multi-sets of subsets of 2^{I_1} . Consider multi-set $\mathcal{A} = [\{\{1\}\}, \{\{1\}\}, \{\{2\}, \{2, 3\}\}, \{\{3\}, \{2, 3\}\}]$. After the following non-trivial elementary compressions, multi-set $\mathcal{B} = [\{\{1\}, \{2, 3\}\}, \{\{1\}, \{2\}, \{3\}, \{2, 3\}\}]$ is obtained.

$$\mathcal{A} = [\{\{1\}\}, \{\{1\}\}, \{\{2\}, \{2, 3\}\}, \{\{3\}, \{2, 3\}\}] \quad (51)$$

$$\geq [\{\{1\}\}, \{\{1\}, \{2\}, \{2, 3\}\}, \{\{3\}, \{2, 3\}\}] = \mathcal{A}' \quad (52)$$

$$\geq [\{\{1\}\}, \{\{1\}, \{2\}, \{3\}, \{2, 3\}\}, \{\{2, 3\}\}] = \mathcal{A}'' \quad (53)$$

$$\geq [\{\{1\}, \{2, 3\}\}, \{\{1\}, \{2\}, \{3\}, \{2, 3\}\}] = \mathcal{B} \quad (54)$$

Therefore, $\mathcal{A} \geq \mathcal{B}$ and step (a) of inequality (50) follows.

Here, we discuss an alternative visual tool. Associate a graph $G_{\mathcal{A}}$ to multi-set \mathcal{A} . Each node of this graph represents one set in multi-set \mathcal{A} , and is labeled by it. Two nodes are connected by an edge if and only if none is a subset of the other. Each time an elementary compression is performed on multi-set \mathcal{A} , a compressed multi-set \mathcal{A}' (with a new graph associated to it) is created. E.g., graphs associated to multi-sets \mathcal{A} , \mathcal{A}' , \mathcal{A}'' , and \mathcal{B} (which

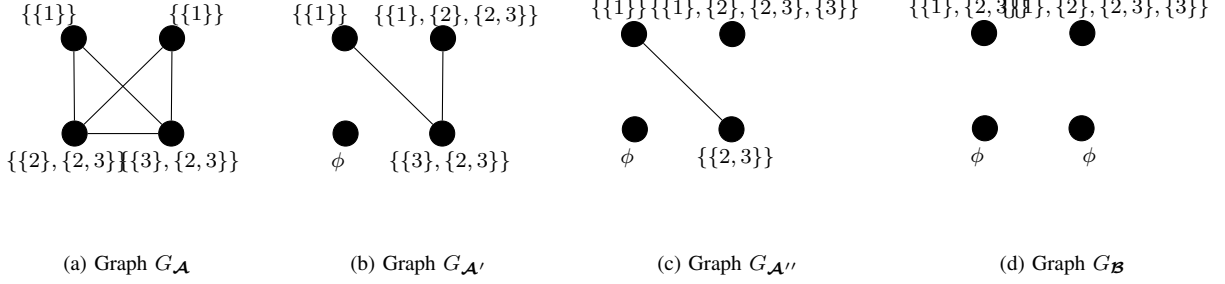


Fig. 7: Graphs associated to multisets \mathcal{A} , \mathcal{A}' , \mathcal{A}'' , \mathcal{B} obtained through the compression that is performed in inequalities (51)-(54)

are all defined in inequalities (51)-(54)) are shown in Figure 7.

For such graphs, we prove that compression reduces the total number of edges in the associated graph.

Lemma 6. *Let $G_{\mathcal{A}}$ denote the graph associated to multi-set \mathcal{A} and $G_{\mathcal{B}}$ denote the graph associated to multi-set \mathcal{B} . Provided that $\mathcal{B} < \mathcal{A}$, the total number of edges of graph $G_{\mathcal{B}}$ is strictly smaller than that of graph $G_{\mathcal{A}}$.*

Proof: We prove that a non-trivial elementary compression over multiset \mathcal{A} strictly reduces the total number of edges in the associated graph. Assume that a non-trivial compression over multi-set \mathcal{A} yields a compressed multi-set \mathcal{A}' , and the compression is performed using two sets \mathcal{A}_i and \mathcal{A}_j . Consider the nodes associated to these two sets and trace all edges connecting them to other nodes of the associated graph throughout the compression. Let \mathcal{A}_k ($\neq \mathcal{A}_i, \mathcal{A}_j$) be an arbitrary node of the associated graph. We show that for any such node, the total number of edges connecting it to \mathcal{A}_i and \mathcal{A}_j does not increase after compression. This is summarized in the following.

- There is an edge $(\mathcal{A}_i, \mathcal{A}_k)$ and an edge $(\mathcal{A}_j, \mathcal{A}_k)$: In this case, no matter what the resulting graph $G_{\mathcal{A}'}$ is after the compression, there cannot be more than two edges connecting \mathcal{A}_k to \mathcal{A}_i and \mathcal{A}_j .
- There is an edge $(\mathcal{A}_i, \mathcal{A}_k)$ but there is no edge $(\mathcal{A}_j, \mathcal{A}_k)$: Since there is no edge between \mathcal{A}_j and \mathcal{A}_k , one of them is a subset of the other.
 - 1) If $\mathcal{A}_j \subseteq \mathcal{A}_k$, then $\mathcal{A}_i \cap \mathcal{A}_j \subseteq \mathcal{A}_k$ and there is therefore no edge between \mathcal{A}_k and $\mathcal{A}_i \cap \mathcal{A}_j$ after the compression.
 - 2) If otherwise $\mathcal{A}_j \supseteq \mathcal{A}_k$, then $\mathcal{A}_i \cup \mathcal{A}_j \supseteq \mathcal{A}_k$ and there is therefore no edge between \mathcal{A}_k and $\mathcal{A}_i \cup \mathcal{A}_j$ after the compression.
- There is no edge $(\mathcal{A}_i, \mathcal{A}_k)$ but an edge $(\mathcal{A}_j, \mathcal{A}_k)$: This case is similar to the previous case.
- There is neither an edge $(\mathcal{A}_i, \mathcal{A}_k)$ nor an edge $(\mathcal{A}_j, \mathcal{A}_k)$: In this case, we have either of the following possibilities.
 - 1) If $\mathcal{A}_i \subseteq \mathcal{A}_k$ and $\mathcal{A}_j \subseteq \mathcal{A}_k$, then both $\mathcal{A}_i \cup \mathcal{A}_j$ and $\mathcal{A}_i \cap \mathcal{A}_j$ are subsets of \mathcal{A}_k and there is no edge connecting

Multiset \mathcal{B}	Multiset $\mathcal{Q} > \mathcal{B}$
$[\dots, \{\{i, j\}^*\}, \{\{i\}^*, \{j\}^*\}, \dots]$	$[\dots, \{\{i\}^*\}, \{\{j\}^*\}, \dots]$
$[\dots, \{\{1, 2, 3\}\}, \{\{i, j\}^*, \{i, k\}^*\}, \dots]$	$[\dots, \{\{i\}^*\}, \{\{j, k\}^*\}, \dots]$
$[\dots, \{\{1, 2, 3\}^*\}, \{\{i, j\}^*, \{i, k\}^*, \{j, k\}^*\}, \dots]$	$[\dots, \{\{i, j\}^*\}, \{\{i, k\}^*\}, \dots]$
$[\dots, \{\{1\}^*, \{2\}^*, \{3\}^*\}, \{\{i\}^*, \{j, k\}^*\}, \dots]$	$[\dots, \{\{i\}^*, \{j\}^*\}, \{\{i\}^*, \{k\}^*\}, \dots]$
$[\dots, \{\{1\}^*, \{2\}^*, \{3\}^*\}, \{\{i, j\}^*, \{i, k\}^*\}, \dots]$	$[\dots, \{\{i\}^*\}, \{\{j\}^*, \{k\}^*\}, \dots]$
$[\dots, \{\{1\}^*, \{2\}^*, \{3\}^*\}, \{\{i, j\}^*, \{i, k\}^*, \{j, k\}^*\}, \dots]$	$[\dots, \{\{i\}^*, \{j\}^*\}, \{\{k\}^*, \{i, j\}^*\}, \dots]$

TABLE I: Non-trivial elementary decompositions for multi-sets of subsets of $2^{\{1,2,3\}}$

- \mathcal{A}_k to $\mathcal{A}_i \cap \mathcal{A}_j$ or $\mathcal{A}_i \cup \mathcal{A}_j$ over $G_{\mathcal{A}'}$, after the compression.
- 2) If $\mathcal{A}_i \subseteq \mathcal{A}_k$ and $\mathcal{A}_j \supseteq \mathcal{A}_k$, then $\mathcal{A}_i \cup \mathcal{A}_j \supseteq \mathcal{A}_k$ and $\mathcal{A}_i \cap \mathcal{A}_j \subseteq \mathcal{A}_k$ and there is therefore no edge connecting \mathcal{A}_k to $\mathcal{A}_i \cap \mathcal{A}_j$ or $\mathcal{A}_i \cup \mathcal{A}_j$ over graph $G_{\mathcal{A}'}$, after the compression.
 - 3) If $\mathcal{A}_i \supseteq \mathcal{A}_k$ and $\mathcal{A}_j \subseteq \mathcal{A}_k$, then similar to the previous case one concludes that there is no edge connecting \mathcal{A}_k to $\mathcal{A}_i \cap \mathcal{A}_j$ or $\mathcal{A}_i \cup \mathcal{A}_j$ over graph $G_{\mathcal{A}'}$.
 - 4) If $\mathcal{A}_i \supseteq \mathcal{A}_k$ and $\mathcal{A}_j \supseteq \mathcal{A}_k$, then both $\mathcal{A}_i \cup \mathcal{A}_j$ and $\mathcal{A}_i \cap \mathcal{A}_j$ are supersets of \mathcal{A}_k and there is therefore no edge connecting \mathcal{A}_k to $\mathcal{A}_i \cap \mathcal{A}_j$ or $\mathcal{A}_i \cup \mathcal{A}_j$ over graph $G_{\mathcal{A}'}$.

Furthermore, since the compression is non-trivial, nodes \mathcal{A}_i and \mathcal{A}_j have been connected over graph $G_{\mathcal{A}}$ and are no longer connected over graph $G_{\mathcal{A}'}$. So, the total number of edges in graph $G_{\mathcal{A}}$ is strictly smaller than $G_{\mathcal{A}'}$, and this concludes the proof. \blacksquare

Define a (*non-trivial*) *decompression* as the inverse act of a (non-trivial) compression. As opposed to compression, a non-trivial decomposition is not always possible using every two elements of a multi-set \mathcal{B} . It is, indeed, not clear whether a multi-set \mathcal{B} is decompressable at all. For example, multi-set $[\{\{2, 3\}, \{1, 2, 3\}\}, \{\{1\}, \{2\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}]$ cannot be non-trivially decompressed; i.e., there exists no multi-set \mathcal{A} such that

$$\mathcal{A} > [\{\{2, 3\}, \{1, 2, 3\}\}, \{\{1\}, \{2\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}]. \quad (55)$$

Table I gives a list of some non-trivial elementary decompositions for multi-sets of subsets of $2^{\{1,2,3\}}$, and i, j, k are permutations of 1, 2, 3.

Although not all multi-sets are decompressable, Lemma 7 below identifies a class of multi-sets of subsets of $2^{\{1,2,3\}}$ that are decompressable.

Lemma 7. *Let \mathcal{B} and \mathcal{A} be multi-sets of subsets of $2^{\{1,2,3\}}$, where \mathcal{B} is of saturated pattern and \mathcal{A} is of standard pattern. If \mathcal{B} and \mathcal{A} are balanced, then a non-trivial elementary decomposition could be performed over multi-set \mathcal{B} unless $\mathcal{B} = \mathcal{A}$.*

Proof: The proof is by showing that for any multi-set \mathcal{B} with the stated assumptions, at least one of the non-trivial elementary decompositions in Table I is doable. This is done by double counting (once in \mathcal{B} and once

in \mathcal{A}) the number of times each subset $S \in 2^{\{1,2,3\}}$ appears in multi-set \mathcal{B} , and showing that no matter what \mathcal{B} and \mathcal{A} are, at least one of the cases of Table I occurs. We defer details of this proof to Appendix C. ■

Lemma 7 shows that a multi-set \mathcal{B} of saturated pattern, which is balanced with a multi-set \mathcal{A} of standard pattern, can be non-trivially decompressed. Let the result of this non-trivial elementary decompression be multi-set \mathcal{Q} . Since the decompressed multi-set \mathcal{Q} is, itself, of saturated pattern and remains balanced with multi-set \mathcal{A} , one can continue decompressing it using Lemma 7 as long as $\mathcal{Q} \neq \mathcal{A}$. This, either ends in an infinite loop, or ends in $\mathcal{Q} = \mathcal{A}$; and the former is ensured not to happen, by Lemma 6.

Lemma 8. *Let \mathcal{B} and \mathcal{A} be multi-sets of subsets of $2^{\{1,2,3\}}$, where \mathcal{B} is of saturated pattern and \mathcal{A} is of standard pattern. If \mathcal{B} and \mathcal{A} are balanced, then \mathcal{B} can be decompressed to \mathcal{A} ; i.e., $\mathcal{A} \geq \mathcal{B}$.*

2) *Converse:* With these tools in hand, we are now ready to prove Theorem 3 which provides a matching outer-bound to the rate region of Theorem 1, when there are three public and many private receivers. The key to proving the converse is the following lemma which we only state here and we defer its proof to Appendix D.

Lemma 9. *Consider the rate region characterization in Theorem 1 (where $I_1 = \{1, 2, 3\}$ and $I_2 = \{4, \dots, K\}$). The constraints given by inequality (20) in Theorem 1 can be replaced by (56) given below, without affecting the rate-region.*

$$\sum_{S \in \mathcal{T}} \alpha_S \geq 0, \quad \forall \mathcal{T} \subseteq 2^I \text{ subset saturated} \quad (56)$$

By Lemma 9, the rate region of Theorem 1 is equivalently given by constraints (56), (21)-(24). We start by finding an outer-bound which looks *similar* to the this inner-bound.

Lemma 10. *Any achievable rate pair (R_1, R_2) satisfies outer-bound constraints (57)-(60) for any given $\epsilon > 0$.*

$$\frac{1}{n} H(\bar{X}_{\mathcal{T}} | W_1) \geq 0 \quad \forall \mathcal{T} \subseteq 2^{I_1} \mathcal{T} \text{ superset saturated} \quad (57)$$

$$R_1 + \frac{1}{n} H(\bar{X}_{\{\{i\}^*\}} | W_1) \leq \sum_{S \in \{\{i\}^*\}} |\mathcal{E}_S| + \epsilon \quad \forall i \in I_1 \quad (58)$$

$$R_2 \leq \frac{1}{n} H(\bar{X}_{\mathcal{T}} | W_1) + \sum_{S \in \mathcal{T}^c} |\mathcal{E}_S^p| + \epsilon \quad \forall \mathcal{T} \subseteq 2^{I_1} \text{ superset saturated}, \forall p \in I_2 \quad (59)$$

$$R_1 + R_2 \leq \sum_{S \subseteq I_1} |\mathcal{E}_S^p| + \epsilon \quad \forall p \in I_2 \quad (60)$$

Notice the similarity of inequalities (57), (58), (59), (60) with constraints (56), (22), (23), (24), respectively. We provide no similar outer-bound for the inner-bound constraint (21) because it is redundant.

Proof: Inequalities (57) hold by positivity of the entropy function. To show inequalities in (58), we bound R_1 for each public receiver $i \in I_1$ as follows.

$$nR_1 \leq H(W_1) \quad (61)$$

$$\leq H(W_1) \pm H(W_1 | \bar{Y}_i) \quad (62)$$

$$\stackrel{(a)}{\leq} I(W_1; \bar{Y}_i) + n\epsilon \quad (63)$$

$$= I(W_1; \bar{X}_{\{\{i\}\star\}}) + n\epsilon \quad (64)$$

$$= H(\bar{X}_{\{\{i\}\star\}}) - H(\bar{X}_{\{\{i\}\star\}}|W_1) + n\epsilon \quad (65)$$

$$\stackrel{(b)}{\leq} n \left(\sum_{S \in \{\{i\}\star\}} |\mathcal{E}_S| \right) - H(\bar{X}_{\{\{i\}\star\}}|W_1) + n\epsilon \quad (66)$$

In the above chain of inequalities, (a) follows by Fano's inequality and (b) follows by cardinality bound of entropy. In a similar manner for each private receiver p we have the following bound on $nR_1 + nR_2$, which proves inequality (60).

$$nR_1 + nR_2 \leq H(W_1, W_2) \quad (67)$$

$$\leq I(W_1, W_2; \bar{X}_{\{\{p\}\star\}}) + n\epsilon \quad (68)$$

$$\leq H(\bar{X}_{\{\{p\}\star\}}^p) + n\epsilon \quad (69)$$

$$\leq n \left(\sum_{S \in \{\{p\}\star\}} |\mathcal{E}_S^p| \right) + n\epsilon \quad (70)$$

Finally, we bound R_2 to obtain inequalities in (59). In the following, $p \in I_2$ and $\mathcal{T} \subseteq 2^{I_1}$.

$$nR_2 \leq H(W_2|W_1) \quad (71)$$

$$\leq H(W_2|W_1) \pm H(W_2|W_1, \bar{Y}_p) \quad (72)$$

$$\stackrel{(a)}{\leq} I(W_2; \bar{Y}_p|W_1) + n\epsilon \quad (73)$$

$$\leq I(W_2; \bar{X}_{\{\{p\}\star\}}^p|W_1) + n\epsilon \quad (74)$$

$$\leq H(\bar{X}_{\{\{p\}\star\}}^p|W_1) + n\epsilon \quad (75)$$

$$\stackrel{(b)}{\leq} H(\bar{X}_{\{\{p\}\star\}}^p, \bar{X}_{\mathcal{T}}|W_1) + n\epsilon \quad (76)$$

$$\leq H(\bar{X}_{\mathcal{T}}|W_1) + H(\bar{X}_{\{\{p\}\star\}}^p|\bar{X}_{\mathcal{T}}, W_1) + n\epsilon \quad (77)$$

$$\stackrel{(c)}{\leq} H(\bar{X}_{\mathcal{T}}|W_1) + H(\bar{X}_{\mathcal{T}^c}^p) + n\epsilon \quad (78)$$

$$\stackrel{(d)}{\leq} H(\bar{X}_{\mathcal{T}}|W_1) + n \left(\sum_{S \in \mathcal{T}^c} |\mathcal{E}_S^p| \right) + n\epsilon \quad (79)$$

In the above chain of inequalities, step (a) follows by Fano's inequality. Step (b) holds for any subset $\mathcal{T} \subseteq 2^{I_1}$ and in particular subsets which are superset saturated. Step (c) follows because we remove the conditioning in the entropy term and increase the right hand side. Step (d) follows by cardinality bound on entropy. ■

The rate region of Theorem 1 can be obtained explicitly by applying Fourier-Motzkin elimination method to (56), (22)-(24) to eliminate parameters α_S . This gives a set of inequalities of the form $m_1 R_1 + m_2 R_2 \leq E$, each obtained by summing potentially multiple copies of constraints (56), (22)-(24), so that all variables α_S , $S \subseteq I_1$, get eliminated. To show a converse for each such inner-bound inequality, $m_1 R_1 + m_2 R_2 \leq E$, take copies of the

corresponding outer-bound constraints (57)-(60) and sum them up to yield an outer-bound inequality of the form

$$\begin{aligned} m_1 R_1 + m_2 R_2 + \frac{1}{n} \sum_{T \in \mathcal{A}} H(\bar{X}_T | W_1) \\ \leq E + \frac{1}{n} \sum_{T \in \mathcal{B}} H(\bar{X}_T | W_1), \end{aligned} \quad (80)$$

where \mathcal{A} is a multi-set of standard pattern and \mathcal{B} is a multi-set of saturated pattern, both consisting of subsets of 2^{I_1} where $I_1 = \{1, 2, 3\}$. Notice that \mathcal{A} and \mathcal{B} are balanced since Fourier-Motzkin elimination ensures that all the α_S 's are eliminated. So by Lemma 8, $\mathcal{B} \leq \mathcal{A}$ and therefore,

$$\sum_{T \in \mathcal{B}} H(\bar{X}_T | W_1) \leq \sum_{T \in \mathcal{A}} H(\bar{X}_T | W_1). \quad (81)$$

Using inequality (81) in the outer-bound inequality (80) concludes the converse to $m_1 R_1 + m_2 R_2 \leq E$.

APPENDIX A

PROOF TO LEMMA 3

We proved equivalency of statement (i) and statement (ii) in Subsection 2 and deferred the proof to equivalency of statements (ii) and (iii) to here:

(ii) \Rightarrow (iii): Assume that a message of rate c could be unicast over the virtual network of Figure 3 (from node A to node B). Therefore, there are c edge-disjoint paths from source node A to sink node B . Each such path matches one of the outgoing edges of source node A to one of the incoming edges of sink node B . We call this, matching M between outgoing edges of the source and incoming edges of the sink, and we note that its size is c . We use this matching to fill the indeterminates of matrix \mathbf{T} with 0 – 1. First of all, note that each column i of matrix \mathbf{T} corresponds to an outgoing edge of the source, say e_j , and each row i of matrix \mathbf{T} corresponds to an incoming edge of the sink, say e'_j , such that entry (i, j) of matrix \mathbf{T} is zero if and only if edges e_j and e'_j cannot be matched. Now, put a 1 in entry (i, j) of matrix \mathbf{T} if edge e_j is matched to edge e'_j over matching M . Since matching M has a size equal c , matrix \mathbf{T} is filled column-fullrank and is given by a permutation of $\mathbb{I}_{c \times c}$.

(iii) \Rightarrow (ii): Assume there is a column fullrank 0 – 1 assignment of matrix \mathbf{T} , which is given by a permutation of $\mathbb{I}_{c \times c}$. Use this assignment to find a matching of size c between the outgoing edges of source node A to incoming edges of sink node B , as we did above. This yields c edge-disjoint paths from node A to node B . Therefore, the maximum flow from source node A to sink node B is at least c , and therefore a message W of rate c could be unicast from source node A to sink node B .

APPENDIX B

PROOF TO LEMMA 5

For simplicity of notation, we give the proof for the case where $m = 2$. Let \mathbf{A} take all its invariants uniformly at random over finite field \mathbb{F} , and let message W_1 be available at receiver p . We prove that message W_2 is decodable (with high probability) if and only if message W_2 could be unicast over the virtual network of Figure 8. In this

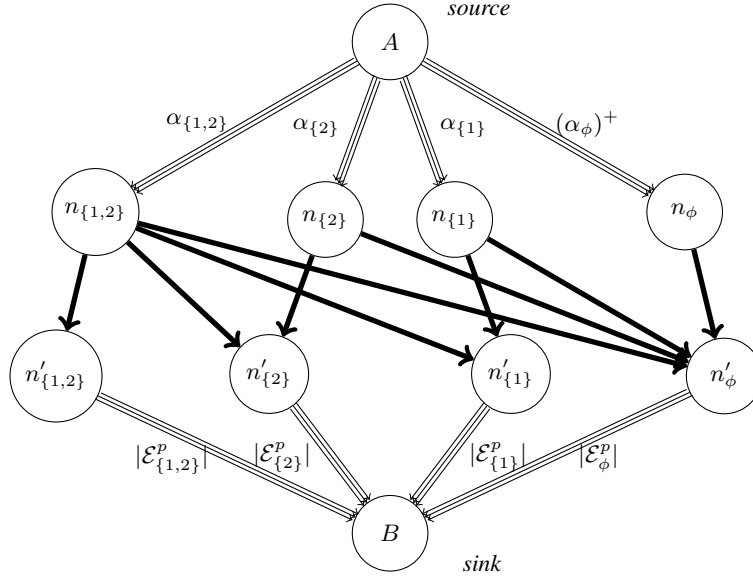


Fig. 8: Source node A communicates a message of rate R_2 to the sink node, B .

network thin edges are of unit and thick edges are of infinite capacity. Since W_1 is available at receiver p , it can construct from $Y_p = \mathbf{A}_p \begin{bmatrix} W_1 \\ W_2 \end{bmatrix}$, a vector $Y'_p = \mathbf{T}'_p W_2$, where \mathbf{T}'_p is the sub-matrix of \mathbf{A}_p which is formed by its last R_2 columns. Furthermore, \mathbf{T}'_p could be written as follows.

$$\mathbf{T}'_p = \begin{matrix} & \begin{matrix} \xleftrightarrow{\alpha_{\{1,2\}}} & \xleftrightarrow{\alpha_{\{1\}}} & \xleftrightarrow{\alpha_{\{2\}}} & \xleftrightarrow{\alpha_{\phi}} \end{matrix} \\ \begin{bmatrix} & 0 & 0 & 0 \\ & & 0 & 0 \\ & 0 & & 0 \\ & & & \end{bmatrix} & \begin{matrix} \updownarrow |\mathcal{E}_{\{1,2\}}^p| \\ \updownarrow |\mathcal{E}_{\{1\}}^p| \\ \updownarrow |\mathcal{E}_{\{2\}}^p| \\ \updownarrow |\mathcal{E}_{\phi}^p| \end{matrix} \end{matrix} \cdot \mathbf{P} \quad (82)$$

Think of matrix \mathbf{P} as the local transfer matrix at source node A . Also, think of the matrix formed by the first $|\mathcal{E}_{\{1,2,3\}}^p|$ rows of \mathbf{T}'_p as the local transfer matrix at intermediate node $n_{\{1,2,3\}}$ and so on. Notice to the equivalence of matrix \mathbf{T}'_p to the transfer matrix imposed by a random linear network coding over the virtual network of Figure 8, and conclude that message W_2 is decodable (with high probability) if and only if message W_2 could be unicast over the virtual network of Figure 8 by random linear network coding. Decodability conditions at receiver p can, therefore, be inferred by finding the min-cut separating nodes A and B over the virtual network of Figure 8. Lemma 4 gives this min-cut by the following expression.

$$\min \left\{ \min_{\substack{\mathcal{T} \subset 2^{I_1} \\ \mathcal{T} \text{ superset saturated}}} \sum_{S \in \mathcal{T}} \alpha_S + \sum_{S \in \mathcal{T}^c} |\mathcal{E}_S^p|, \sum_{S \in 2^I_1, S \neq \phi} \alpha_S + (\alpha_{\phi})^+ \right\} \quad (83)$$

One can easily verify that R_2 is smaller than the expression in (83), provided that inequalities in (23) hold.

APPENDIX C
PROOF TO LEMMA 7

Let \mathcal{B} be a multiset of $2^{\{1,2,3\}}$ with saturated pattern, \mathcal{A} be a multi-set of $2^{\{1,2,3\}}$ with standard pattern, and \mathcal{A} and \mathcal{B} be balanced and such that $\mathcal{B} \neq \mathcal{A}$. We prove that no matter what \mathcal{A} and \mathcal{B} are, at least one of the cases of Table I occurs, and therefore a non-trivial elementary decompression is feasible.

Let us first count, in two different ways (once in \mathcal{B} and once in \mathcal{A}), the number of times a sets $S \subseteq I_1$ appears in sets of multi-sets \mathcal{B} and \mathcal{A} . First of all Define n_S , $S \subseteq I_1$ to be multiplicity of sets $T \in \mathcal{A}$ that contain set S . One observes (from the standard pattern of multi-set \mathcal{A}) that $n_S = \sum_{i \in S} n_{\{i\}}$. Similarly, define m_T to be multiplicity of a set T in multi-set \mathcal{B} . For simplicity of notation we use $m_{T \cup}$, to denote multiplicity of all of sets S in \mathcal{B} of the form $S \supseteq T$.

Since multi-sets \mathcal{A} and \mathcal{B} are balanced, multiplicity of sets in \mathcal{A} containing a set S is equal to multiplicity of sets in \mathcal{B} containing it. Thus, counting multiplicity of sets in \mathcal{A} and \mathcal{B} which contains $\{i\}$ and $\{i, j\}$, we obtain the following relationship. In the following, we assume i, j, k to be permutations of 1, 2, 3.

$$n_{\{i\}} = m_{\{\{i\} \star\} \cup} \quad (84)$$

$$n_{\{i, j\}} = m_{\{\{i\} \star\} \cup} + m_{\{\{j\} \star\} \cup} - m_{\{\{i\} \star, \{j\} \star\} \cup} + m_{\{\{i, j\} \star\} \cup} \quad (85)$$

Since $n_{\{i, j\}} = n_{\{i\}} + n_{\{j\}}$, we conclude from (84) and (85) the following equation.

$$m_{\{\{i\} \star, \{j\} \star\} \cup} = m_{\{\{i, j\} \star\} \cup}. \quad (86)$$

Similarly, counting multiplicity of sets in \mathcal{A} and \mathcal{B} which contains $\{1, 2, 3\}$, we reach to the following equation.

$$\begin{aligned} n_{\{1,2,3\}} &= m_{\{\{1\} \star\} \cup} + m_{\{\{2\} \star\} \cup} + m_{\{\{3\} \star\} \cup} + m_{\{\{1,2\} \star\} \cup} + m_{\{\{1,3\} \star\} \cup} + m_{\{\{2,3\} \star\} \cup} + \\ &+ m_{\{\{1,2,3\} \star\} \cup} - m_{\{\{1\} \star, \{2\} \star\} \cup} - m_{\{\{1\} \star, \{3\} \star\} \cup} - m_{\{\{2\} \star, \{3\} \star\} \cup} - m_{\{\{1\} \star, \{2,3\} \star\} \cup} + \\ &- m_{\{\{2\} \star, \{1,3\} \star\} \cup} - m_{\{\{3\} \star, \{1,2\} \star\} \cup} - m_{\{\{1,2\} \star, \{1,3\} \star\} \cup} - m_{\{\{1,2\} \star, \{2,3\} \star\} \cup} + \\ &- m_{\{\{1,3\} \star, \{2,3\} \star\} \cup} + m_{\{\{1,2\} \star, \{1,3\} \star, \{2,3\} \star\} \cup} + m_{\{\{1\} \star, \{2\} \star, \{3\} \star\} \cup} \end{aligned} \quad (87)$$

Using $n_{\{1,2,3\}} = n_{\{1\}} + n_{\{2\}} + n_{\{3\}}$, equation (84) and equation (86) in equation (87), one obtains the following equation.

$$\begin{aligned} m_{\{\{1,2,3\} \star\} \cup} + m_{\{\{1\} \star, \{2\} \star, \{3\} \star\} \cup} &= m_{\{\{1\} \star, \{2,3\} \star\} \cup} + m_{\{\{2\} \star, \{1,3\} \star\} \cup} + m_{\{\{3\} \star, \{1,2\} \star\} \cup} + \\ &+ m_{\{\{1,2\} \star, \{1,3\} \star\} \cup} + m_{\{\{1,2\} \star, \{2,3\} \star\} \cup} + m_{\{\{1,3\} \star, \{2,3\} \star\} \cup} \\ &- m_{\{\{1,2\} \star, \{1,3\} \star, \{2,3\} \star\} \cup} \end{aligned} \quad (88)$$

Now we write each $m_{\mathcal{T} \cup}$ in terms of $\sum_{\substack{S \in \mathcal{B} \\ S \supseteq \mathcal{T}}} m_S$ to derive the equation of our interest.

$$\begin{aligned}
m_{\{1,2,3\}^*} + m_{\{1\}^*, \{2\}^*, \{3\}^*} &= m_{\{1\}^*, \{2,3\}^*} + m_{\{2\}^*, \{1,3\}^*} + m_{\{3\}^*, \{1,2\}^*} + m_{\{1,2\}^*, \{1,3\}^*} + \\
&\quad + m_{\{1,2\}^*, \{1,3\}^*, \{2,3\}^*} + m_{\{1,2\}^*, \{2,3\}^*} + m_{\{1,2\}^*, \{1,3\}^*, \{2,3\}^*} + \\
&\quad + m_{\{1,3\}^*, \{2,3\}^*} + m_{\{1,2\}^*, \{1,3\}^*, \{2,3\}^*} - m_{\{1,2\}^*, \{1,3\}^*, \{2,3\}^*} \\
&= m_{\{1\}^*, \{2,3\}^*} + m_{\{2\}^*, \{1,3\}^*} + m_{\{3\}^*, \{1,2\}^*} + m_{\{1,2\}^*, \{1,3\}^*} + \\
&\quad + m_{\{1,2\}^*, \{2,3\}^*} + m_{\{1,3\}^*, \{2,3\}^*} + 2m_{\{1,2\}^*, \{1,3\}^*, \{2,3\}^*} \tag{89}
\end{aligned}$$

Observe from equality (89) that if there is a non-zero term, $m_{\mathcal{T}_1}$, on the left hand, there is at least one other non-zero term, $m_{\mathcal{T}_2}$, on the right hand of the equality. No matter what \mathcal{T}_1 and \mathcal{T}_2 are, see that we are in one of the decompression cases we studied in the beginning of the proof. If both sides of equality (89) are zero, then one concludes that $m_{\{i\}^*, \{j\}^* \cup} = m_{\{i\}^*, \{j\}^*}$ and $m_{\{i,j\}^* \cup} = m_{\{i,j\}^*}$ and therefore, by equation (86), we have another equation of interest.

$$m_{\{i\}, \{j\}} = m_{\{i,j\}} \tag{90}$$

Again, if $m_{\{i\}, \{j\}}$ is none-zero so is $m_{\{i,j\}}$, and we are back to one of the cases described in Table I.

We have proved that a non-trivial elementary decomposition is possible unless all terms in (89) and (90) are zero, and all terms in (89) and (90) are zero only if $\mathcal{B} = \mathcal{A}$ which is assumed not to be the case.

APPENDIX D PROOF TO LEMMA 9

Let us call the rate region characterized in Theorem 1 (when $I_1 = \{1, 2, 3\}$), region \mathcal{R}_1 and the rate region obtained from relaxing inequality (20) to inequality (56) (when $I_1 = \{1, 2, 3\}$), region \mathcal{R}_2 . Clearly, $\mathcal{R}_1 \subseteq \mathcal{R}_2$. It is therefore sufficient to show that $\mathcal{R}_2 \subseteq \mathcal{R}_1$. Both rate regions \mathcal{R}_1 and \mathcal{R}_2 are in terms of feasibility problems. In this sense, rate pair (R_1, R_2) belongs to \mathcal{R}_1 if and only if feasibility problem 1 (characterized by inequalities (20)-(24)) is feasible. Similarly, rate pair (R_1, R_2) belongs to \mathcal{R}_1 if and only if feasibility problem 2 (characterized by inequalities (56),(21)-(24)) is feasible. In order to show that $\mathcal{R}_2 \subseteq \mathcal{R}_1$, we show that if (R_1, R_2) is such that there exists a solution, α_S , $S \subseteq I_1$, to feasibility problem 2, then there also exists a solution α'_S , $S \subseteq I_1$, to feasibility problem 1. Note that region \mathcal{R}_1 varies from \mathcal{R}_2 only in the non-negativity constraints on parameters α'_S , $\phi \neq S \subseteq I_1$. The goal is construct parameters α'_S from parameters α_S such that besides satisfying constraints (21)-(24), they all become non-negative except for α_ϕ . This is done in the following three steps.

We prove existence of solution α'_S , $S \subseteq 2^{I_1}$, by construction and recursively. To give an overview of the proof, we start from a solution to feasibility problem 1, α_S , $S \subseteq I_1$, and at each step we propose a solution α'_S , $S \subseteq I_1$, which is still a solution to feasibility problem 1 but is *strictly less negative* (excluding α_ϕ). So after enough number of steps, we end up with a set of parameters α'_S , $S \subseteq I_1$, that satisfies (21)-(24) and also satisfies the non-negativity constraints in (20).

1. **Choose a non-negative $\alpha'_{\{1,2,3\}}$:** Set $\alpha'_{\{1,2,3\}} = \alpha_{\{1,2,3\}}$. Verify that all α'_S , $S \subseteq \{1, 2, 3\}$, satisfy (21) to (24) and (56).
2. **Choose non-negative parameters $\alpha'_{\{i,j\}}$, $i, j \in \{1, 2, 3\}$:** Without loss of generality take the following three cases.
 - (a) $\alpha_{\{1,2\}} < 0$ and $\alpha_{\{1,3\}} < 0$ and $\alpha_{\{2,3\}} < 0$:
 Set $\alpha'_{\{1,2,3\}} = \alpha_{\{1,2,3\}} + \alpha_{\{1,2\}} + \alpha_{\{1,3\}} + \alpha_{\{2,3\}}$, $\alpha'_{\{1,2\}} = \alpha'_{\{1,3\}} = \alpha'_{\{2,3\}} = 0$, $\alpha'_{\{i\}} = \alpha_{\{i\}}$ for $i = 1, 2, 3$, and $\alpha'_\phi = \alpha_\phi$. Verify that all α'_S , $S \subseteq \{1, 2, 3\}$, satisfy (21) to (24) and (56).
 - (b) $\alpha_{\{1,2\}} < 0$ and $\alpha_{\{1,3\}} < 0$:
 set $\alpha'_{\{1,2,3\}} = \alpha_{\{1,2,3\}} + \alpha_{\{1,2\}} + \alpha_{\{1,3\}}$, $\alpha'_{\{1,2\}} = \alpha'_{\{1,3\}} = 0$, $\alpha'_{\{2,3\}} = \alpha_{\{2,3\}}$, $\alpha'_{\{i\}} = \alpha_{\{i\}}$ for $i = 1, 2, 3$, and $\alpha'_\phi = \alpha_\phi$. Verify that all α'_S , $S \subseteq \{1, 2, 3\}$, satisfy (21) to (24) and (56).
 - (c) $\alpha_{\{1,2\}} < 0$:
 Set $\alpha'_{\{1,2,3\}} = \alpha_{\{1,2,3\}} + \alpha_{\{1,2\}} \geq 0$, $\alpha'_{\{1,2\}} = 0$, $\alpha'_{\{1,3\}} = \alpha_{\{1,3\}}$, $\alpha'_{\{2,3\}} = \alpha_{\{2,3\}}$, $\alpha'_{\{i\}} = \alpha_{\{i\}}$ for $i = 1, 2, 3$, and $\alpha'_\phi = \alpha_\phi$. Verify that all α'_S , $S \subseteq \{1, 2, 3\}$, satisfy (21) to (24) and (56).
3. **Choose non-negative parameters $\alpha'_{\{i\}}$, $i \in \{1, 2, 3\}$:** Repeat the following procedure for each $\alpha'_i < 0$ until all $\alpha'_{\{i\}}$, $i = 1, 2, 3$, are non-negative. δ is assumed a small enough positive number.
 - (a) if $\alpha'_{\{i,j\}}, \alpha'_{\{i,k\}} > 0$:
 Set $\alpha'_{\{i\}} = \alpha'_{\{i\}} + \delta$, $\alpha'_{\{i,j\}} = \alpha'_{\{i,j\}} - \delta$, $\alpha'_{\{i,k\}} = \alpha'_{\{i,k\}} - \delta$, $\alpha'_{\{1,2,3\}} = \alpha'_{\{1,2,3\}} + \delta$, and keep the rest of α'_S 's unchanged. Verify that all α'_S , $S \subseteq \{1, 2, 3\}$, satisfy (21) to (24) and (56).
 - (b) if $\alpha'_{\{i,j\}} = 0$, $\alpha'_{\{i,k\}} > 0$:
 Set $\alpha'_{\{i\}} = \alpha'_{\{i\}} + \delta$, $\alpha'_{\{i,k\}} = \alpha'_{\{i,k\}} - \delta$, and keep the rest of α'_S 's unchanged. Verify that all α'_S , $S \subseteq \{1, 2, 3\}$, satisfy (21) to (24) and (56).
 - (c) if $\alpha'_{\{i,j\}} > 0$, $\alpha'_{\{i,k\}} = 0$:
 Set $\alpha'_{\{i\}} = \alpha'_{\{i\}} + \delta$, $\alpha'_{\{i,j\}} = \alpha'_{\{i,j\}} - \delta$, and keep the rest of α'_S 's unchanged. Verify that all α'_S , $S \subseteq \{1, 2, 3\}$, satisfy (21) to (24) and (56).
 - (d) if $\alpha'_{\{i,j\}} = 0$, $\alpha'_{\{i,k\}} = 0$:
 Set $\alpha'_{\{i\}} = \alpha'_{\{i\}} + \delta$, $\alpha'_{\{1,2,3\}} = \alpha'_{\{1,2,3\}} - \delta$, and keep the rest of α'_S 's unchanged. Verify that all α'_S , $S \subseteq \{1, 2, 3\}$, satisfy (21) to (24) and (56).

Note that after step 1, one obtains a solution to feasibility problem 2, in which $\alpha_{\{1,2,3\}} \geq 0$. Then, after step 2, one obtains a solution to feasibility problem 2, in which $\alpha_{\{i,j\}} \geq 0$ for all $i, j \in \{1, 2, 3\}$, and $\alpha_{\{1,2,3\}}$ is still non-negative. In step 3, at each iteration, a solution is constructed to feasibility problem 2, where $\alpha_{\{1,2\}}, \alpha_{\{1,3\}}, \alpha_{\{2,3\}}, \alpha_{\{1,2,3\}}$ all remain non-negative and at the same time, one negative $\alpha_{\{i\}}$ is increased. So after step 3, all parameters α_S , $\phi \neq S \subseteq \{1, 2, 3\}$ become non-negative, and therefore this is the solution to feasibility problem 1 that we were looking for.

REFERENCES

- [1] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, "Network information flow," *Information Theory, IEEE Transactions on*, vol. 46, no. 4, pp. 1204 –1216, jul 2000.
- [2] S.-Y. Li, R. Yeung, and N. Cai, "Linear network coding," *Information Theory, IEEE Transactions on*, vol. 49, no. 2, pp. 371 –381, feb. 2003.
- [3] R. Koetter and M. Medard, "An algebraic approach to network coding," *Networking, IEEE/ACM Transactions on*, vol. 11, no. 5, pp. 782 – 795, oct. 2003.
- [4] S. Jaggi, P. Sanders, P. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen, "Polynomial time algorithms for multicast network code construction," *Information Theory, IEEE Transactions on*, vol. 51, no. 6, pp. 1973 – 1982, june 2005.
- [5] T. Ho, R. Koetter, M. Medard, D. Karger, and M. Effros, "The benefits of coding over routing in a randomized setting," in *Information Theory, 2003. Proceedings. IEEE International Symposium on*, july 2003, p. 442.
- [6] A. Ramamoorthy and R. D. Wesel, "The single source two terminal network with network coding," *CoRR*, vol. abs/0908.2847, 2009.
- [7] C. Ngai and R. Yeung, "Multisource network coding with two sinks," in *Communications, Circuits and Systems, 2004. ICCCAS 2004. 2004 International Conference on*, vol. 1, june 2004, pp. 34 – 37 Vol.1.
- [8] E. Erez and M. Feder, "Capacity region and network codes for two receivers multicast with private and common data," in *Workshop on Coding, Cryptography and Combinatorics*, 2003.
- [9] S. Gheorghiu, S. Saeedi Bidokhti, C. Fragouli, and A. Toledo, "Degraded multicasting with network coding over the combination network," in *IEEE International Symposium on Network Coding*, 2011.
- [10] C. K. Ngai and R. Yeung, "Network coding gain of combination networks," in *Information Theory Workshop, 2004. IEEE*, oct. 2004, pp. 283 – 287.
- [11] P. Balister and B. Bollobás, "Projections, Entropy and Sumsets," *ArXiv e-prints*, Nov. 2007.